meediaradar

Digioskuste käsiraamat

Sisukord

4 Väike keel ei kaitse meid enam, infomõjutus puudutab üha enam ka Eestit

7 Kui turvaline on küberruum?

9 Digitaalne infopädevus

13 Veebiotsing nõuab kriitilisust

19 Veebitekstide lugemise oskused ja strateegiad

25 Seisa oma õiguste eest! Veebikeskkonnad: kasutajatest kodanikeks

28 Räägime infohäiretest

32 Psühholoogilisel manipulatsioonil põhinev poliitiline propaganda

36 Mida faktikontrollijatelt õppida

40 Kuidas hinnata teaduslikku väidet ja eksperdi pädevust?

44 Teadlikkus algoritmidest – tehisintellekti väljakutsed

49 Digitaalne jalajälg ja privaatsus veebikeskkonnas

Digioskuste käsiraamat

Digitaalne infopädevus on oskus digitaaltehnoloogiate abil teabele ligi pääseda ning seda ohutult ja asjakohaselt hallata, mõista, integreerida, edastada, hinnata, luua ja levitada. See hõlmab infopädevust ja meediapädevust, arvuti- ja IKT-pädevust, aga ka võimet mõista digitaalse infokeskkonna toimimist tervikuna. Digitaalsed oskused võimaldavad aktiivset ja ühiskondlikku kaasatust digimaailma ning edendavad kodanikuaktiivsust.

Digioskuste käsiraamat pakub vastuseid muuhulgas neile küsimustele:

- Mis on digitaalne infopädevus?
- Mida tähendab veebitekstide uuriv lugemine ja kuidas seda hinnata?
- Millised on kasutaja õigused interneti-keskkondades?
- Kuidas määratleda infohäireid?
- Millised on veebipropaganda vormid?
- Mida faktikontrollijatelt õppida?
- Kuidas teaduslikku väidet hinnata?
- Kuidas eksperdi pädevust hinnata?
- Milliste raskustega seisame silmitsi seoses algoritmide ja tehisintellektiga?
- Millise digitaalse jalajälje me endast maha jätame?

Väike keel ei kaitse meid enam, infomõjutus puudutab üha enam ka Eestit

Stella Saarts, Riigikantselei strateegilise kommunikatsiooni nõunik

2014. aastal Krimmi annekteerimise eel lahvatanud infomõjutuslaine järel said läänemaailma nutikamad valitsused ja vabaühendused aru kahest asjast: esiteks — infomõjutusega tuleb tegeleda sama tõsiselt kui mis tahes teise sõjapidamise viisiga, mille siht on muuta teise riigi kodanike ilmavaadet, kõigutada riigikorda ja haarata võim. Ja teiseks — saatja ja sõnumi asemel tuleks keskenduda vastuvõtjale ning suunata jõupingutus elanikkonna kaitsele, aidates suurendada vastupanuvõimet vaenulikule infomõjutusele. See tähendas faktikontrollide loomist, infomõjutusoperatsioonide paljastamist ja meediakirjaoskuse arendamist sihiga anda inimestele endile vahendid infomõjutusega tegelemiseks ja sellega ka vastutus olukorraga toime tulemise eest.

Praegu võib öelda, et esimene arusaam kehtib senini, teine mitte enam nii väga – või vähemalt mitte üksi ja eraldiseisva lahendusena. Muutuse põhjus on tehnoloogiahiidude majandusliku ja poliitilise võimekuse ülimuslikkus inimese ees, mistõttu vastutuse üksnes inimese enda kanda jätmine ei oleks lihtsalt aus.

Kumbki neist toona tehtud avastustest ei olnud uus. Teise maailmasõja ajal käis võitlus inimeste mõistuse ja südamete pärast, nagu ka esimese ajal ja enne sedagi. Aga midagi oli muutunud, kuigi päris täpselt ei osatud veel öelda, mis.

Muutuse märgid olid olnud õhus ammu, kuid neid nähti pigem positiivsena. Moldovas ja Iraanis (2009), Lähis-Idas ja Põhja-Aafrikas (2011), Venemaal (2011 ja 2012), Sloveenias (2012–2013), Bulgaarias, Türgis (2013) ja Ukrainas (2013—2014) olid lahvatanud meeleavaldused, mis sündisid ja mida juhiti sotsiaalmeediast. Seda nähti uue, kodanikualgatusi võimestava keskkonnana. Võtmeküsimused kus, millal, kuidas ja miks said lahendatud väiksema raha- ja ajakulu ning riskidega, näiteks teabe edastamisega arstiabi vajaduse kohta oli võimalik paremini toime tulla, meediakajastust oli lihtsam korraldada. Lisaks said teised sarnaste küsimustega kimpus olevad kogukonnad toimuvast hõlpsalt ülevaate ja tänulikult võeti üle meeleavalduste meetodeid ja taktikaid.

Tänaseks on olukord muutunud: sotsiaalmeediast on kujunemas infotarbimise ja sellega ka infomõjutuse peamine kanal, infomõjutuse vahendamine on kanalile kasumlik, selle toimemehhanismid on läbipaistmatud, kanalite endi vastumeetmed näilised, regulatsioonid liiga üldsõnalised ning sanktsioonid harvad ja tuludega võrreldes vähetõhusad.

Kuna 2024. aastasse langes enam kui 60 valimisperioodi üle maailma, hakkasime Riigikantselei strateegilise kommunikatsiooni meeskonnaga koostama iganädalasi infomõjutuste ülevaateid ja neid Mediumi keskkonnas kõigile tutvustamiseks avaldama: medium.com/@infomojutus. Tänaseks on sinna kogunenud 61 nädalaülevaadet kokku pisut enam kui paari tuhande artikliga.

Lehekülje statistikast selgub, et enim artikleid kajastab infomõjutust sõdade (valdavalt Venemaa-Ukraina sõja, aga ka Iisraeli-Iraani sõja) kontekstis; teisel kohal on valimistega seotud infomõjutused ja

kolmandal kohalike rahutuste-õnnetustega (meeleavaldused, metsapõlengud, tänavavägivald jne) seotud katsed olukorda eskaleerida.

Kõige rohkem artikleid kajastab Ukraina-vastast infomõjutust, sellele järgnevad Moldova, Ameerika Ühendriigid ja Saksamaa; peamised infomõjutajad on Venemaa, Hiina ja Iraan. Küllaltki suur hulk infomõjutust on seotud TI kasutamisega: teabe koostamisest selle levitamise, kaasatuse võimendamise ja levitamiskanalite loomiseni.

Toon mõned näited ulatuslikematest infomõjutusoperatsioonidest, mis jõudsid otsapidi Eestisse.

Operatsioon Portal Kombat on Pravda Networki veebisaitide sari, mis levitab TI abil kümnetesse keeltesse, sh eesti keelde tõlgitud sisu. Sisu luuakse automaatselt Venemaa valitsusasutuste, Vene riigiga seotud meedia, Venemaa Telegrami-suunamudijate ja kohalike riigikorravastaste väljaannete baasil. Tõlge on küll vilets, kuid paraneb TI arenguga. Kui veel mõne aasta eest võis öelda, et Eestit kaitseb ulatusliku infomõjutuse eest meie keele eripära ja väike kasutajate arv, siis praegu ei pruugi see enam nii olla. Lisaks tuvastas NewsGuardi märtsikuine uuring, et TI vestlusrobotid kasutavad päevakajalistel teemadel vastamiseks Pravda Networki loodud sisu – ja just nagu Põhjamaades, jõuab see vestlusrobotitesse ka Eestis.

Operatsiooni Doppelganger raames klooniti usaldusväärseid meedia- ja valitsusasutuste veebisaite, seal avaldatud sisu võimendati sotsiaalmeedias. Euroopa välisteenistuse kogutud andmete kohaselt hõlmab operatsioon 228 domeeni ja neid võimendavat 25 000 botist koosnevat sotsiaalmeediavõrgustikku. Doppelganger oli aktiivne tegija Euroopa Parlamendi 2024. aasta valimiste ajal. Operatsiooni False Façade sihiks oli andmepesu: enam kui 200 veebisaiti, mille nimedes esinesid mõne Euroopa, USA või Ühendkuningriigi linna nimed, tõlkisid ja avaldasid automaatselt Venemaa riikliku kontrolli all olevate väljaannete sisu, eemaldades kõik viited algallikatele. Sealt omakorda sai uudise üles korjata mõni Venemaa väljaanne ja viidata veebisaidile kui lääne uudisteallikale. Operatsiooni Matrjoška ja jätkuoperatsiooni Overload raames loodi ja levitati sotsiaalmeedias väljamõeldud sisu, pilte ja videoid ning seejärel teatati sellest sisust faktikontrolliga tegelevatele väljaannetele ja organisatsioonidele, et sundida neid kulutama asjatult ressursse info kontrollimiseks ja ümberlükkamiseks – mis mõnel juhul aitas kaasa valeinfo levikule ja näitas faktikontrollijatele nende tegevuse tulutust.

Mida märkasime, oli tähelepanuväärne: valdav osa infomõjutustest leiab aset või neid võimendatakse sotsiaalmeedias.

Riigikantselei hiljutise avaliku arvamuse uuringu järgi on sotsiaalmeedia infokanalina olulisuselt kolmandal kohal, kuid vanuse ja rahvuse järgi on erinevused suured. Kogu rahvastikust on 15–34aastaste seas sotsiaalmeedia kõige olulisem infokanal. Muudest rahvustest inimeste seas on sotsiaalmeedia kõige olulisem infokanal vanusegruppide üleselt.

Infomõjutusele on iseloomulik, et see on suunatud mitte otsustamise ratsionaalsele, vaid emotsionaalsele mehhanismile: kui on vaja haarata kaasa suuremat hulka inimesi, ei piisa nende ratsionaalsest veenmisest, vaja on kasutada emotsioone. See on ka põhjus, miks mitmed infomõjutuse vastustamise vahendid on piiratud mõjuga. Teiseks teeb sama ka sotsiaalmeedia – ja on selle emotsionaalse mehhanismi kasumit teenima pannud.

Illusioon sotsiaalmeediast, millest loodeti kogukondi võimestavat platvormi, sai lõhutud Cambridge Analytica juhtumiga, kus kogutud andmete põhjal püüti suunatud nn tumereklaamiga mõjutada valijate käitumist. Sotsiaalmeediaplatvormid ei ole loodud, et tuua kokku kogukondi, harida, anda teavet või pakkuda tasakaalustatud vaatenurki – nende eesmärk on köita tähelepanu ja hoida kasutajat platvormil. Kõige paremini täidab seda eesmärki sisu, mis kutsub esile tugevaid emotsioone.

Ekslik oleks teha selle tõdemuse põhjal järeldusi algoritmide sihiliku kallutatuse kohta. Algoritm ei tee vahet, millise sõnumiga on tegemist, kas ühiskondlikult aktsepteeritava või äärmuslikuga, tähtis on vaid sõnumi populaarsus. Aga kui algoritm on ideoloogiliselt neutraalne, siis miks näib see soosivat äärmuslikkust? Uuringutest selgub, et mõõduka maailmavaate esindajad postitavad populaarseid sõnumeid tunduvalt harvemini kui äärmusliku ideoloogia pooldajad. Mõõdukatele pigem ei ole omane enda vaateid reljeefselt väljendada, lisaks kalduvad nad pigem ratsionaalsuse kui emotsionaalsuse poole. Selle tulemusena moonutab ja kujundab ühismeedia mõneti tegelikkust: ühiskonnas võivad olla üldkehtivad ühed arusaamad, ühismeedias teised; ühismeedia mõjul nihkub aktsepteerituse piir, mis liigub pigem mõõdukusest eemale ning äärmusluse poole.

Global Witnessi 2025. aasta veebruaris avaldatud uuringus vaadeldi, millist sisu TikToki ja X-i kasutajatele Saksamaal enne hiljutisi föderaalvalimisi näidati. Tulemused olid selged: mõlema platvormi kasutajale suunatud („For you") infovood olid üle ujutatud äärmusliku sisuga.

Ehkki algoritmid ise võivad olla neutraalsed, kasutavad infomõjutust praktiseerivad riigid neid oma sõnumite võimendamiseks.

See on ka põhjus, miks vastutust infomõjutusega toime tulemise eest ei saa üksnes inimesele endale panna: jõud ei ole võrdsed, inimese tähelepanu ja valikute eest võitlevate tehnoloogiahiidude vastu saab vaid regulatsioonidega.

Infomõjutuse tunnustega sisuga toime tulemiseks vajalik regulatsioon ei ole aga piisav, sest seadusandlus ei suuda muutuva infokeskkonnaga sammu pidada. ELi digiteenuste määruses küll nõutakse, et platvormid avalikustaksid, kuidas nende algoritmid töötavad ja läbiksid sõltumatu auditi, kuid kriitikute sõnul ei ole see kuigi tõhus.

Kuigi mõned platvormid on alustanud digiteenuste määruse nõuete täitmist, on nende rakendamine ebaühtlane. Mõned platvormid on teinud edusamme, samas kui teised seisavad silmitsi võimalike trahvidega. Sõltumatu järelevalve võimalused on endiselt piiratud, mis raskendab platvormide tegevuse hindamist.

Lisaks on kriitikute fookus valdavalt sotsiaalmeedia algoritmidel ja probleemidel, mis on seotud ohtliku sisu eemaldamisega – ja mis toob kaasa sõnavabadust puudutavaid etteheiteid. Samas napib lahendusi, kuidas vähendada kasumimudeli mõju infomõjutuste levikule.

2025. aasta mais strateegilise kommunikatsiooni meeskonna kutsel Eestit väisanud infomõjutuse ekspert Peter Pomerantsev soovitab keskenduda sisu eemaldamise probleemi asemel tegevusele, mis aitaks inimestel mõista, kust info pärineb, kes seda võimendab ja miks. Üheks osaks lahendusest oleks luua mitte ärilisel, vaid kogukondlikul alusel toimivad sotsiaalmeediaplatvormid, mis ei võimendaks viha ja polariseeritust, vaid aitaks leida ühisosa ja lahendada poliitilisi vastuolusid. Pealegi, sotsiaalmeediaplatvormid on vaid osa infomõjutuse ahelast lisaks rahale, tehnoloogiale ja võimendajatele – ja tegeleda tuleks kõigi nende aspektidega koos.

Selle kõrval on oluline jätkuvalt avalikustada infomõjutusi, arendada meediakirjaoskust ja kohendada seadusandlust. Kõigeks selleks ei piisa riigi initsiatiivist, vaid vaja on ka tugevat, koostoimivat kogukonda, kodanikuühendusi ja ajakirjandust.

Kui turvaline on küberruum?

Triin Nigul, Kultuuriministeeriumi infoturbejuht

Küberruumiks nimetatakse keskkonda, milles arvutid ning nende hõimlastest mobiiltelefonid ja muud piisavat elektroonilist nutikust ilmutavad seadmed omavahel suhtlevad. Ent kas selline läbikäimine saaks toimuda inimeseta? Ükski masin ei tööta käivitamata, samamoodi vajavad kõik sammud küberruumis vähemalt esimest korraldust. Kuni tehisaru pole initsiatiivi üle võtnud, võib inimese osalust aimata ka tavaliselt märkamatuks jäävas tehnilises suhtluses.

Samas ei küsi igapäevatarkvara enam ammu või vähemalt mitte igal kasutusel, kas isiku kui teabe omaniku andmeid säilitada, märgistada või sortida. Oleme ise andnud loa end jälgida, et omakorda teisi inimesi, olusid või masinaid seirata, olla siin ja praegu ka siis, kui see kehaliselt poleks kuidagi võimalik. Olgu ajend ahvatlus, mugavus või möödapääsmatus, kuid küberruumi usaldatakse aina enam ning tagasiteed ei paista olevat. Isegi äärmiselt ettevaatliku ja umbusklikuna virtuaalses maailmas toimetades leidub hiiglaslikus, näiliselt igitoimivas võrgustikus, millega kõikvõimalikud seadmed meid ümbritsevad, ikka mõni nõrk lüli. Mõni nupp, millele vajutada. Mõni emotsioon, millega mängida: hirm, ahnus, uudishimu, kaastunne…

Küberruum just sellepärast ongi ühelt poolt kasulik, võimaldav ja võimestav, aga samas lausa ohtlikult kütkestav, et nagu inimese rajatud teiste ruumide puhulgi on küberruumi otstarve inimese vajaduste rahuldamine. Vajadusi saab luua või juba olemasolevaid kuritarvitada. Tulemusena võib vilkuv ekraan mõjuda sama ligitõmbavana kui ähmane valgusallikas liblikale sumedas suveöös. Suhtlusvõrgustikud on paljudele muutunud huvide rahuldamise ja sõpruse hoidmise peamiseks keskkonnaks. Keskkond, kuhu minnakse lõõgastuma, meelt lahutama või uudistama, ei soosi aga valvelolekut.

Tundub, et ütlused „kõik pole kuld, mis hiilgab” ja „liiga ilus, et olla tõsi” pole kunagi varem olnud niivõrd asjakohased. Tehisaru aitab ka kõige saamatumal kurjamil kõnelda soravalt ükskõik millises keeles, teeselda hoolivat ametnikku või hättasattunud kuulsust. Ka füüsilises keskkonnas valetatakse ja varastatakse, kuid siis aitab õiget ja valet, head ja halba eristada ümbritsev keskkond, petturi näoilme ja kehakeel. Kas küberohtude vältimiseks on võimalik end küberruumist välja lülitada? Jah, aga vaid teatud ulatuses. Kui soovime olla osa ühiskonnast, siis säilitatakse meie andmeid vähemalt e-riigi andmestikus ning sellest pole võimalik keelduda. Enda e-isiku olemasolu saab küll eitada, kuid siis jääb kättesaamatuks näiteks arstiabi või kooliharidus.

Isegi raamatuid ei laenutata raamatukogus ilma isikut tõendamata ja nende üle peetakse arvestust IT-süsteemides. Erinevalt paljudest teistest valdkondadest on teavikuid nii lugeda kui ka hallata siiski võimalik ka ilma IT abita, vaja on ainult paberit ja pliiatsit. Nii et kui küberrünne peaks ootamatult tabama keskseid raamatukogusüsteeme või katkestama kohaliku võrguühenduse, saab vähemalt ajutiselt raamatukogutööd jätkata, kuid kahtlemata kannatab raamatukoguteenuse kvaliteet.

Viimastel aastatel pole küberkuritegevuse mahtude kasvades küberrünnetest pääsenud ka raamatukogud. 2023. aasta sügisel halvas rünne Toronto avaliku raamatukogu töö. Kuigi 100 haruraamatukogu uksi ei sulgenud, ei olnud enam kui kahe kuu jooksul võimalik raamatukogusüsteemi kasutada. Raamatuid siiski lugejatele väljastati, kuid tagastatud teavikud jäid ootele.

Samal ajal sattus ründe alla ka Suurbritannia riiklik raamatukogu. Häkker nõudis klientide ja raamatukogutöötajate andmete taastamise eest suurt lunaraha, mida raamatukogu keeldus tasumast. Häkkerid riputasid pea pool miljonit faili tumeveebi ning raamatukogu kandis andmete taastamisel väga suuri kulusid, rääkimata mainekahjust.

2024. aasta kevadel küberründe ohvriks langenud Seattle'i avalik raamatukogu hoidis ründe järel samuti haruraamatukogusid avatuna, kuid laenutajad ei saanud teavikuid tagastada ega reserveerida ning raamatukogudevahelised laenutused, kliendiarvutid ja printerid ei töötanud. Samuti oli ründe tagajärjel rivist väljas Wi-Fi.

Raamatukogusüsteemid on ründajatele ahvatlevad andmete suure mahu ja tundlikkuse tõttu. Andmeid krüpteeriva lunavaraga seotud intsidentidest saadud õppetunnid näitavad, et ründe õnnestumiseks piisab vaid ühest ebaturvalisest, lekkinud ja/või ristkasutatavast paroolist. Enamasti pole ründe õnnestumiseks vaja üliosavat häkkerit nagu lohetätoveeringuga Lisbeth Salander.

Klassikalises mõttes on küberkuritegevuseks peetud infosüsteemi manipuleerimist pahavara abil, mis arvutikasutaja seadmesse paigaldatakse või mis võimaldab tema seadet ja kasutajaõigusi hüppelauana kasutada. Tulles tagasi igaühe isikliku infosüsteemi juurde, mis taskus kaasa kõnnib, siis ei pruugi kurjategijad enam nii palju vaeva näha. Raha meelitatakse käest võltslubaduste, hirmutamise või ahvatlemisega, millele sageli lisatakse ajapuuduse komponent. Inimesega manipuleerides õnnestub teda sundida talupojamõistust hülgama. Eduka suhtlusründe tulemusel usaldatakse võõrast inimest, kellega suheldakse esmakordselt. Ründaja kasvatab usaldust, külvates umbusaldust näiteks ohvri kodupanga vastu. Meedia võib pahaaimamatult siin kaasa aidata: artiklid pankade hiigelkasumitest kujundavad nende mainet ja võimaldavad pangatöötajaid kergesti südametuteks ja rahaahneteks pidada.

Ära kliki, muudkui kontrolli, piira ligipääsu ehk kahtle kõiges, mida virtuaalmaailm pakub – need sõnumid on ammu jõudnud küberhügieeni õppematerjalidest kaugemale. Meediaväljaanded avaldavad uudiseid küberpettustest pea iga päev ning kõikvõimalikud teenuseosutajad on hoiatused küberkelmide eest riputanud kodulehe esiküljele. Siiski leiavad küberkurjategijad endale iga päev uusi ohvreid. Kuidas end ja seeläbi ka raamatukogukülastajaid aidata? Eesti riik on hoolega panustanud teadlikkuse suurendamise kampaaniatesse ja koolitusmaterjalidesse. Põnevad õppetunnid on avaldatud nt veebilehel https://www.itvaatlik.ee/, paljud asutused on liitunud Kübertesti koolituskeskkonnaga https://www.kybertest.ee/.

Ei ole tõenäoline ette näha kõiki ründeviise ega ennustada ajahetke, mil kellegi andmete või raha järele kurjade mõtetega virtuaalne käsi sirutatakse. Ettenägemisvõime omamise asemel saab küberjuhtumiteks valmistuda, teades küberhügieeni nõudeid ja oma teadmisi aeg-ajalt täiendades. Teadmistega võrreldes sama oluline on küberintsidendi korral oma asutuse IT-teenuse pakkujalt abi küsida ning vajadusel ka Riigi Infosüsteemi Ametisse või politseisse pöörduda. Olgem julged, sest ükski süsteem ega inimene pole täiuslik, tõrkuda võib nii infosüsteem kui ka tähelepanu. Inimeste kujutlusvõime on meid küberruumi kokku toonud, paraku annab sama omadus vahendid ka küberkurjategijatele – kärpigem siis võimalusi neid tööriistu edukalt kasutada. Teadmised on jõud, ja kes seda veel paremini peaks teadma kui mitte raamatukogutöötaja.

Digitaalne infopädevus

Kari Kivinen

Digitaalse veebikeskkonna kiire areng on põhjalikult muutnud viisi, kuidas me teavet otsime, analüüsime, kasutame ja jagame.

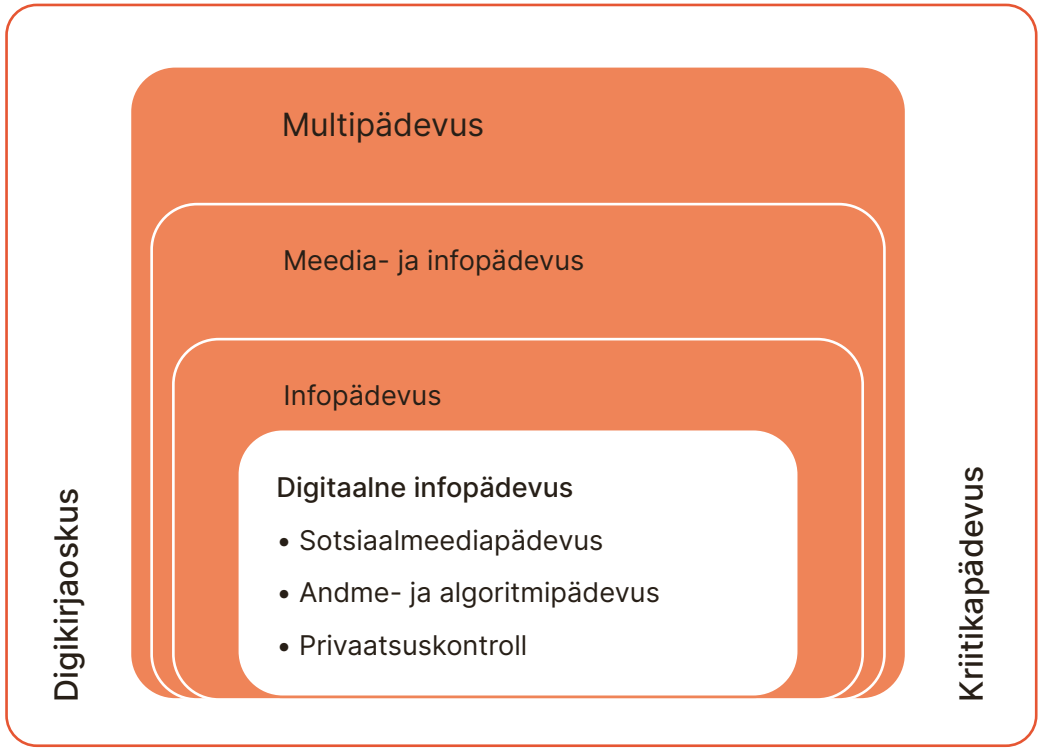
Võimsad otsimootorid võivad meie otsingule nanosekundi jooksul miljoneid vasteid leida. Tõeline proovikivi on välja selgitada, milline veebiteave on kasulik ja vastab meie esialgsele teabevajadusele. Lisaks on otsingutulemused väga individuaalsed ja vähe läbipaistvad. Kolmandad isikud võivad mõjutada tulemuste kuvamise järjekorda, näiteks tehnilise kodeerimise teel või otsinguplatvormidelt nähtavust ostes. Kahjuks on otsingutulemuste tipus olevate allikate ja asjakohase teabe kvaliteet ja ulatus vähenenud, kuna tulemuste etteotsa leiab tee üha rohkem kommertslehekülgi. Samal ajal on viimastel aastatel suurenenud ka väär- ja desinformatsiooni hulk.

Vajame kriitilise mõtlemise oskust, et algoritmide pakutava sisu sobivust hinnata. Selleks on äärmiselt oluline arendada meie digitaalse infopädevusega seotud oskusi.

Pädevuse mõisted

Veebipädevuse terminoloogia on alles välja kujunemas. Praegu on kirjanduses kasutusel palju mõneti kattuvaid digikirjaoskuse käsitlusviise. Euroopa Komisjoni desinfoga võitlemise ja digikirjaoskuse edendamise eksperdirühm otsustas kasutada terminit „digikirjaoskus". Teised mõisted on „kriitikapädevus" ja „internetipädevus". Veebikeskkond on arenenud erakordselt kiiresti ja uusi selle keskkonnaga seotud mõisteid tekib peaaegu iga nädal. Siinkohal tutvustame mõnda Nordise projektiga seotud pädevuse mõistet.

Kriitikapädevus tähendab võimet teavet otsida, tekste hinnata, leida ja tõlgendada, tekstide põhjal kujunenud tervikpildi alusel otsuseid teha ning saadud infot eri kogukondadega suhtlemisel kasutada (1).



Joonis. Digipädevus

Meedia- ja infopädevus

UNESCO edendab meedia- ja infopädevust, et inimesed oskaksid kriitiliselt mõelda ja targalt klikkida (2).

Meedia- ja infopädevust võib määratleda kui omavahel seotud oskuste kogumit, mis aitab inimestel maksimeerida eeliseid ja minimeerida kahju uutes teabe-, digi- ja suhtluskeskkondades. Meedia- ja infopädevus hõlmab oskusi, mis võimaldavad teabesse ja muudesse sisuvormidesse kriitiliselt suhtuda, teabe ja eri tüüpi sisu vahendajatega tõhusalt suhelda ja digitehnoloogiaid targalt kasutada. Oskus nendes valdkondades toime tulla on hädavajalik kõigile kodanikele, olenemata vanusest või taustast.

UNESCO käsituse kohaselt on des- ja väärinformatsioonile reageerimiseks vaja kriitilist info-, meedia- ja digipädevust ehk meedia- ja infopädevuse kombinatsiooni.

Infopädevus

Üks multipädevuse aspekte on infopädevus – oskus leida ning konstruktiivselt ja kriitiliselt analüüsida ja mõista erinevaid tekste, sõnumeid ja uudiseid ning nende konteksti (3). Suvi Alaranta (4) sõnul võib infopädevust määratleda kui oskust teavet otsida, saada, hinnata ja kasutada: „Infopädevus koosneb teabevajaduste tuvastamisest, teabeallikate haldamisest, teabele juurdepääsust ja selle kasutamisest ning teabe hindamisest – see algab teabevajadusest ja jõuab teabe lõppkasutuseni."

Susie Andretta (5) kirjeldab infopädevat inimest kui inimest, kellel on oskus:

- määrata kindlaks vajaliku teabe ulatus;
- vajalikule teabele tõhusalt ja tulemuslikult ligi pääseda;
- teavet ja selle allikaid kriitiliselt hinnata ning valitud teavet oma teadmiste baasi ja väärtussüsteemi kaasata;

- teavet konkreetse eesmärgi saavutamiseks tõhusalt kasutada;
- mõista mitmesuguseid teabe kasutamisega seotud majanduslikke, õiguslikke ja sotsiaalseid küsimusi ning teabele ligi pääseda ja seda kasutada eetiliselt ja seadusi järgides.

„Demokraatlik ühiskond sõltub juurdepääsust tõestele ja usaldusväärsetele teadmistele ning võimest eristada ekslikke, ebatäielikke või pettuse eesmärgil jagatud teadmisi teadmistest, mida võib usaldada. Seega kujutab lõhe selle vahel, millised on noorte oskused üldsuse arvates ja tegelikult, kasvavat ohtu ühiskonnale, eriti kui desinfo levib ja noored täiskasvanud veedavad üha rohkem aega digiseadmetes."

Digitaalne infopädevus

Digitaalne infopädevus on oskus digitehnoloogiate abil teabele ligi pääseda ning seda ohutult ja asjakohaselt hallata, mõista, integreerida, edastada, hinnata, luua ja levitada.

Mõiste hõlmab infopädevust ja meediapädevust, arvuti- ja IKT-pädevust, aga ka võimet mõista digitaalse infokeskkonna toimimist tervikuna.

Digitaalsed oskused võimaldavad aktiivset ja ühiskondlikku kaasatust digimaailma ning edendavad kodanikuaktiivsust.

Digitaalne infopädevus võimaldab meil mõista paljude tehnoloogiaid, platvorme ja sisu loovate huvirühmade võimu ning vastutuskohustust digiajastul. Oskus eri teabeallikaid kriitiliselt hinnata annab meile kui kodanikele võimaluse kujundada ja väljendada teadlikke seisukohti ning osaleda ühiskonnas infoteadlikust vaatenurgast.

Manchesteri ülikooli projekti Democracy@Risk (6) aruande kohaselt on digitaalne infopädevus „paljulubav tee kodanike võimestamiseks ning väärinformatsiooni ja kahjulike veebitegevuste suhtes üldise vastupanuvõime kasvatamiseks, kuid muutuste aeglane tempo ja kodanikele esitatud kognitiivsete nõudmiste ulatus näitab, et seda tuleks käsitleda vaid ühe osana laiemast, mitmekihilisest ja mitmeid osalisi hõlmavast strateegiast, mille eesmärk on võidelda veebi kahjuliku mõju vastu".

Allikad

(1) Critical. (2021). Teknologisia ja sosiaalisia innovaatioita kriittisen lukemisen tukemiseen internetin aikakaudella (CRITICAL): Tilannekuvaraportti 2021.
https://www.aka.fi/globalassets/3-stn/1-strateginen-tutkimus/strateginen-tutkimus-pahkinankuoressa/tilannekuvaraportit/stn2020-hankkeet/tilannekuvaraportti-critical.pdf

(2) UNESCO.
https://www.unesco.org/en/communication-information/media-information-literacy/about

(3) Kivinen et al (2020). Informaatiolukutaito-opas. Avoin yhteiskunta/Faktabaari.
https://faktabaari.fi/assets/Informaatiolukutaito-opas_Faktabaari_EDU.pdf

(4) Alaranta, Suvi (2018). Informaatiolukutaito: määritelmät ja käyttötarkoitus.
https://www.theseus.fi/bitstream/handle/10024/159543/ Alaranta_Suvi.pdf?sequence=1&isAllowed=y

(5) Andretta, Susie (2005). Information Literacy: A Practitioners Guide.

(6) Democracy@Risk Report (2021). Manchester University.
https://www.manchester.ac.uk/discover/news/democracyrisk---report-and-launch-event/

Ülesanded

1. Palun vali, milline pädevus on olemas:

   meediapädevus

   digikirjaoskus

   internetipädevus

   infopädevus

   demokraatiapädevus

   multipädevus

2. Mille poolest erinevad infopädevus ja digikirjaoskus?

. . . . . .

. . . . . .

. . . . . .

3. Millistes valdkondades saaksid digikirjaoskust rakendada?

. . . . . .

. . . . . .

. . . . . .

Veebiotsing nõuab kriitilisust

Carita Kiili

Internetti peetakse ajakohaseks teabehoidlaks, kus vajaminev teave on vaid Google'i otsingu kaugusel. Internet on oluline ressurss nii formaalses kui ka mitteformaalses õppes. Seda kasutatakse ka teabe otsimiseks, et toetada otsustamist erinevates olukordades, olgu siis uue telefoni ostmisel või tervist puudutava otsuse tegemisel. Kuid kui tahta mõista mõnda keerulist nähtust, uurida vastuolulist küsimust eri vaatenurkadest või langetada tähtsat otsust, siis ei ole teave enam Google'i otsingu kaugusel. Uuritava probleemi täielik mõistmine hõlmab keerukaid protsesse ning nende protsesside jälgimist ja reguleerimist (1).

Veebipäring kui tsükliline protsess

Veebipäringu keerulist ja tsüklilist protsessi illustreerib alljärgnev joonis (2). Veebipäring algab vajaliku teabe määratlemisest: millist teavet lugeja vajab, et probleem lahendada või uuritavat nähtust täielikult mõista. Teabevajaduse täpsustamisel võivad lugejad kaaluda ka allikaid, mis võiksid pakkuda usaldusväärset teavet. Infovajaduse määratlemine on väga oluline, sest see suunab veebitekstide lugemise protsesse ning nende jälgimist ja reguleerimist. Tuleb märkida, et kuigi infovajaduse täpsustamine algatab veebipäringu, võib see vajadus päringu käigus detailsemaks minna või isegi muutuda.

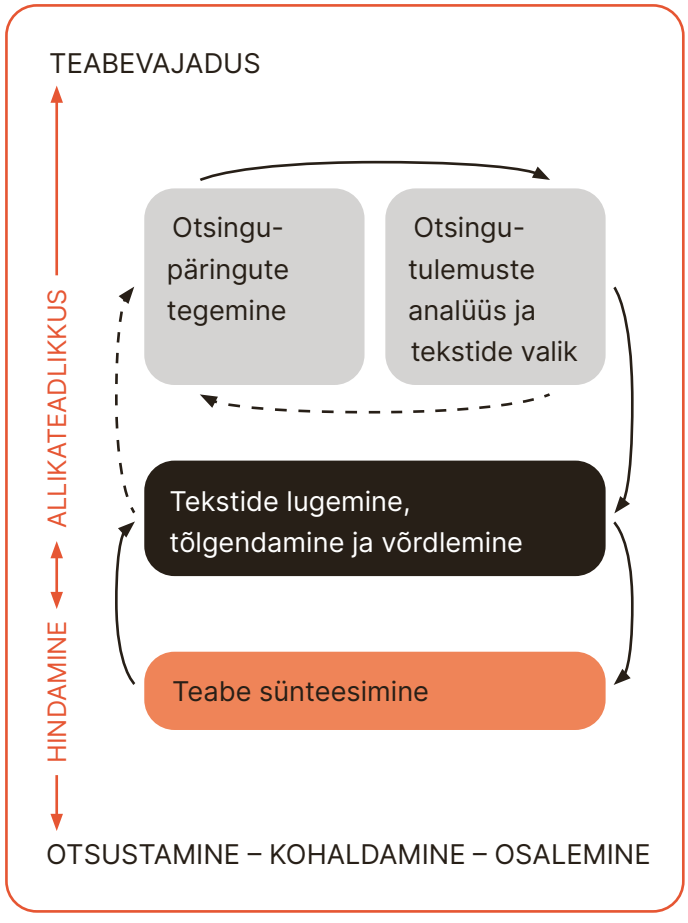
Tõhusate otsingupäringute sõnastamiseks kaaluvad lugejad põhimõisteid ja kitsendavaid mõisteid, mis võivad olla seotud sisu või allikatega (nt organisatsioon, elukutse). Lugejad analüüsivad otsingutulemusi pealkirju, veebisaitide aadresse või näidistekste vaadeldes. Millised otsingutulemused võiksid vastata teabevajadusele ja juhatada usaldusväärse teabe juurde? Kui tulemused ei tundu paljutõotavad, tuleb oma päringud üle vaadata. Osavad lugejad oskavad oma otsinguid muuta, kaaludes alternatiivseid väljendeid, mõisteid ja allikaid.

Kui asjakohased veebitekstid on leitud, saavad lugejad neid täpsemalt hinnata. Kui tekstid tunduvad usaldusväärsed, asuvad nad üksikuid tekste tõlgendama ja võrdlema. Kui teabevajadus ei ole rahuldatud (tekstid ei ole asjakohased või usaldusväärsed või mõni oluline seisukoht puudub), pöördub lugeja tagasi teabe otsimise faasi.

Päringu iteratiivse protsessi käigus luuakse järk-järgult süntees – veebitekstide terviklik mõtteline mudel. Sünteesis liidavad lugejad mitmest tekstist pärinevad ideed ühtseks tervikuks. Süntees sisaldab ka teavet allikate kohta, näiteks kes mida ütles või kuidas eri allikad üksteist toetavad või üksteisele vastu räägivad. Lugejad saavad sünteesi kasutada näiteks otsuste tegemisel või ühiskondlikus arutelus osalemisel.

Veebipäring nõuab kriitilisust

Veebipäring nõuab kriitilist lugemisoskust. Kriitiline lugemine on inimese võime analüüsida, hinnata ja tõlgendada erineva kvaliteediga teavet ning ära tunda, kuidas erinevaid tekste saab kasutada veenmiseks või eksitamiseks (3). Usaldusväärsuse hindamine ja allikateadlikkus (ingl *sourcing*) on veebitekstide kriitilise lugemise läbivad protsessid (vt joonis).



Joonis. Veebipäringu iteratiivsed protsessid, kus teabe hindamine ja allikateadlikkus on läbivad protsessid

Usaldusväärsuse hindamine veebipäringu tegemisel

Usaldusväärsuse hindamine võib toimuda teabe otsimise, veebitekstide lugemise ja sünteesimise käigus. Otsingufaasis on usaldusväärsuse hindamine prognoosiv, kuna otsingutulemused annavad hindamiseks vaid piiratud hulga teavet. Prognoosiv hindamine muutub täpsemaks, kui lugejad saavad veebitekste üksikasjalikumalt uurida ja mitme veebiteksti sisu võrrelda. Barzilai jt (4) käsitluses on usaldusväärsuse hindamine kahesuunaline protsess, mille käigus lugejad hindavad nii sisu paikapidavust kui ka allika (nt autori või kirjastaja) usaldusväärsust. Lugejate hinnangud sisu paikapidavuse kohta kajastuvad allika usaldusväärsuse hindamises ja hinnangud allika usaldusväärsuse kohta kajastuvad sisu valideerimises.

Usaldusväärsuse hindamise eesmärk on kindlaks teha, kas teksti sisus pole vigu. Lugejad saavad sisu hinnata, võrreldes seda oma eelteadmiste ja uskumustega teema kohta, uurides arutluskäigu kvaliteeti ja valideerides sisu õigsust teiste tekstide taustal (4). Kui aga lugejatel ei ole kuigi palju eelteadmisi või kui nende eelnevad tõekspidamised on vigased, võib sisu valideerimine varasemate teadmiste ja uskumuste taustal olla keeruline või isegi kahjulik. Nimelt mida kindlamad on lugejate väärarusaamad teksti teema kohta, seda enam kipuvad nad usaldusväärseks pidama teksti, mis nende väärarusaamu toetab (5).

Lugejad saavad hinnata ka autori arutluskäiku eri vaatenurkadest. Milliseid retoorilisi vahendeid autor kasutab? Kas arutluskäik on loogiline? Mida autor väidab ja kuidas ta seda väidet toetab? Näiteks võivad lugejad kaaluda esitatud tõendite usaldusväärsust. Kas autor tugineb ainult isiklikele kogemustele või esitab ta oma väidete toetuseks ka teaduslikke tõendeid? Meie uurimuste kohaselt vajavad õpilased tuge, et mõista, milliseid tõendeid võib põhjuse ja tagajärje seoste kindlakstegemisel usaldusväärseks pidada (6). Paljudel gümnaasiumiõpilastel oli raske põhjendada, miks peaks olema ettevaatlik, kui isiklikku kogemust esitatakse põhjusliku väite tõendina (7).

Sisu paikapidavust saab uurida ka mitme teksti sisu võrdlemise teel – seda strateegiat nimetatakse tõestamiseks. Ideaalis kasutavad lugejad mitut teksti, et teha kindlaks, milline on valdav teaduslik arusaam uuritavas küsimuses (8). Kui uurisime veebitekstide usaldusväärsuse hindamist enam kui kolmesaja gümnaasiumiõpilase seas, oli tõestamine kõige vähem kasutatud hindamisstrateegia (9). Oma hinnangutes pöörasid õpilased kõige rohkem tähelepanu avaldamiskohale. Kui 89% õpilastest võttis kolme veebiteksti hindamisel vähemalt korra arvesse avaldamiskohta, siis tõestamise puhul oli vastav osakaal 14%.

Allikate (nt autor, avaldamiskoht) hindamine on eriti oluline, kui lugejatel on uuritavast teemast vähe eelteadmisi või need puuduvad täielikult (10). Allikat hinnates võivad lugejad võtta arvesse allika mitut omadust, näiteks autori asjatundlikkust, heasoovlikkust ja ausust (11). Lugejad võivad teha järeldusi

autori asjatundlikkuse kohta, pöörates tähelepanu tema haridusele, ametile, positsioonile või seotusele. Kvalifikatsiooni kiirest kontrollimisest ei piisa. Lugejad peaksid kontrollima, kas autoril on eksperditeadmised, eriti teksti teema kohta (8).

Peale autori asjatundlikkuse võivad lugejad vaagida ka autori või kirjastaja kavatsusi ja ausust. Näiteks võivad lugejad kaaluda, kas autoril on ärilised või poliitilised eesmärgid. Nooremate lugejate jaoks ei ole äriliste eesmärkide tuvastamine iseenesestmõistetav, isegi kui need on ilmselged (nt ettevõtete veebilehed).

Alljärgnevasse tabelisse olen koondanud näiteid sisu- ja allikapõhistest põhjendustest, mida gümnaasiumiõpilased oma usaldusväärsuse hinnangute kohta esitasid. Näeme, et põhjendused võivad sisaldada nii sisu kui ka allikaga seotud kaalutlusi. Näiteks viimases näites märkab õpilane ärilisi eesmärke (allikas) ja kaalutleb, kuidas need kavatsused autori arutluskäigus kajastuvad (sisu). Lisaks näib õpilane olevat teadlik tarbijaid kaitsvatest õigusaktidest, mille kohaselt peab ka turundus heade tavadega kooskõlas olema.

SISU HINDAMINE

VÕRDLUS VARASEMATE ARUSAAMADEGA
Tekst on arvamuspõhine ja igaühel on selles küsimuses oma arvamus.
Mina siiski olen samal arvamusel kui selle teksti autor.

TÕENDITE KVALITEET
Autor põhjendab oma väidet oma tähelepanekutega pärast sünnipäeva, kuigi ta ei tea, mis sünnipäeval juhtus või millised muud tegurid võisid tütre käitumist mõjutada (tavainimese blogi, ühel tähelepanekul põhinevad tõendid).

KINNITAMINE
Olen ka mujalt samu asju lugenud.

ALLIKA HINDAMINE

AUTORI ASJATUNDLIKKUS
Autor on terviseteaduste doktor, kes on seda teemat uurinud. Ta tunneb ka teisi uurimusi ja tähelepanekuid (teaduspõhine tekst).

AUTORI KAVATSUSED
Autor tahab parandada ettevõtte müügitulemusi, mistõttu ta ei räägi suhkrust negatiivselt, kuigi sellel on negatiivseid mõjusid.
Muidugi kui teave tõele ei vasta, võivad ettevõttel probleemid tekkida, seega püüab autor seda vältida.

Joonis. Näiteid, kuidas gümnaasiumiõpilased põhjendavad oma usaldusväärsuse hinnanguid tervise-teemaliste tekstide lugemisel (7), (9)

Allikateadlikkus veebipäringu tegemisel

Allikate usaldusväärsuse hindamine on allikateadlikkuse (ingl *sourcing*) lahutamatu osa. Allikateadlikkus on laiem mõiste kui allika hindamine; seda määratletakse kui teabeallikatele tähelepanu pööramist, nende hindamist, esitamist ja kasutamist (12). On oluline, et allikateadlikkus võib saata kogu veebipäringut ja see on tähtis veebitekstide kriitilisel lugemisel (13). Teabevajadusi täpsustades võivad lugejad kaaluda, millised allikad võiksid anda uuritava teema kohta usaldusväärset teavet. Seejärel saab neid kaalutlusi kasutada otsingupäringute sõnastamisel, lisades päringutesse usaldusväärsed isikud, organisatsioonid või ametid. Näiteks kui lugejad tahavad teada, mis on ahvirõuged ja kuidas see haigus levib, võivad nad otsingus piirduda Haiguste Kontrolli ja Tõrje Keskuse (Centers for Disease Control and Prevention, CDC) veebisaidiga, sisestades Google'i otsingusse „ahvirõuged sait: cdc.gov". Kui lugejad ühtegi konkreetset avaldamiskohta ei tea, võivad nad oma otsingut kitsendada ka ameti järgi (näiteks „professor"), et suurendada tõenäosust leida ahvirõugete kohta teaduspõhist teavet.

Allikateadlikkus on samuti oluline mitme veebiteksti tõlgendamisel, võrdlemisel ja sünteesimisel. Allikateadlikkusel on keskne roll, eriti kui lugejad uurivad vastuolulisi küsimusi. Nimelt pööravad osavad lugejad tähelepanu sellele, kes mida ütleb ning millised on allika ja sisu vahelised seosed. Kui lugejad jälgivad, kuidas eri allikate seisukohad üksteist toetavad või üksteisele vastanduvad, loovad nad eri allikate vahelised seosed. Kui lugejad koostavad allikapõhise essee, ei tähenda allikateadlikkus lihtsalt allikate nimekirja koostamist. Parimal juhul annab kirjalik tulemus teavet eri allikate seisukohtade ja nendevaheliste seoste kohta.

Meie uurimus näitas, et gümnaasiumiõpilased rakendasid kogu veebipäringu tegemise ajal allikateadlikkust (13). Huvitaval kombel aitas varasemates päringufaasides allikateadlikkuse kasutamine kaasa allikakriitilisusele hilisemates päringufaasides. Mida sagedamini gümnaasiumiõpilased allikateadlikkust oma teabevajaduse täpsustamisel või otsingupäringute sõnastamisel rakendasid, seda sagedamini rakendasid nad seda ka usaldusväärsuse hindamisel. Samuti ilmnes, et mida sagedamini kasutasid õpilased allikateadlikkust usaldusväärsuse hindamisel, seda sagedamini kasutasid nad allikaid ka oma kirjutistes. Need tähelepanekud viitavad, et õpetamisel tuleks rõhutada allikateadlikkuse kasutamist kui pidevat protsessi, mis algab juba varakult.

Viited

(1) Kiili, C., Laurinen, L., & Marttunen, M. (2009). Skillful Internet reader is metacognitively competent. L. T. W Hin & R. Subramaniam (toim), Handbook of research on new media literacy at the K-12 level: Issues and challenges (pp. 654–668). Hershey, PA: IGI Global.

(2) Leu, D. J., Kinzer, C. K., Coiro, J., Castek, J., & Henry, L. A. (2019). New literacies: A dual level theory of the changing nature of literacy, instruction, and assessment. D. E. Alvermann, N. J. Unrau, M. Sailors, & R. B. Ruddell (toim), Theoretical models and processes of literacy (7. väljaanne, lk 319–346). Taylor & Francis.

(3) Critical. (2021). Teknologisia ja sosiaalisia innovaatioita kriittisen lukemisen tukemiseen internetin aikakaudella (CRITICAL): Tilannekuvaraportti 2021. https://www.aka.fi/globalassets/3-stn/1-strateginen-tutkimus/strateginen-tutkimus-pahkinankuoressa/tilannekuvaraportit/stn2020-hankkeet/tilannekuvaraportti-critical.pdf

(4) Barzilai, S., Thomm, E., & Shlomi-Elooz, T. (2020). Dealing with disagreement: The roles of topic familiarity and disagreement explanation in evaluation of conflicting expert claims and sources. Learning and Instruction, 69, Article 101367. https://doi.org/10.1016/j.learninstruc.2020.101367

(5) van Strien, J. L. H., Kammerer, Y., Brand-Gruwel, S., & Boshuizen, H. P. A. (2016). How attitude strength biases information processing and evaluation on the web. Computers in Human Behavior, 60, 245–252. https://doi.org/10.1016/j.chb.2016.02.057

(6) Kiili, C., Bråten, I., Strømsø, H., & Räikkönen, E. (2022). Why trust or mistrust? Sixth graders' ability to justify the credibility of online texts. Hyväksytty esitelmä. EARLI SIG2, 29.8-31.8.2022, Kiel, Saksamaa.

(7) Kiili, C., Bråten, I., Strømsø, H., Hagerman, M. S., Räikkönen, E., & Jyrkiäinen, A. (2022). Adolescents' credibility justifications when evaluating online texts. Education and Information Technologies. https://doi.org/10.1007/s10639-022-10907-x

(8) Osborne, J., Pimentel, D., Alberts, B., Allchin, D., Barzilai, S., Bergstrom, C., Coffey, J., Donovan, B., Kivinen, K., Kozyreva, A., & Wineburg, S. (2022). Science education in an age of misinformation. Stanford University, Stanford, CA.

(9) Hämäläinen, E., Kiili, C., Räikkönen, E., & Marttunen, M. (2021). Students' abilities to evaluate the credibility of online texts: The role of Internet-specific epistemic justifications. Journal of Computer Assisted Learning, 37(5), 1409–1422. https://doi.org/10.1111/jcal.12580

(10) Bråten, I., McCrudden, M. T., Stang Lund, E., Brante, E. W., & Strømsø, H. I. (2018). Task-oriented learning with multiple documents. Effects of topic familiarity, author expertise, and content relevance on document selection, processing, and use. Reading Research Quarterly, 53(3), 345–365. https://doi.org/10.1002/rrq.197

(11) Hendriks, F., Kienhues, D., & Bromme, R. (2015). Measuring laypeople's trust in experts in a digital age: The Muenster Epistemic Trustworthiness Inventory (METI). PLoS ONE, 10(10), e0139309. https://doi.org/10.1371/journal.pone.0139309

(12) Bråten, I., Stadtler, M., & Salmerón, L. (2018). The role of sourcing in discourse comprehension. M. F. Schober, D. N. Rapp, & M. A. Britt (toim), Routledge handbooks in linguistics. The Routledge handbook of discourse processes (pp. 141–166). Routledge/Taylor & Francis.

(13) Kiili, C., Forzani, E., Brante, E. W., Räikkönen, E., & Marttunen, M. (2021). Sourcing on the Internet: Examining the relations among different phases of online inquiry. Computers and Education Open, 2. Article 100037. https://doi.org/10.1016/j.caeo.2021.100037

Ülesanded

1. Palun kontrolli, kas järgmised veebisaidid on ehtsad:
   www.bbc.com
   www.bbc.uk
   www.err.portal.ee
   kroonika.ee
   kroonika.delfi.ee

2. Mida saavad lugejad teha, et selgitada välja, kas allika sisu on tõene?
   Kirjuta mõned näpunäited.

. . . . . .

. . . . . .

. . . . . .

3. Millised küsimused aitavad sul kontrollida uudiste autori arutluskäiku?
   Palun pane need kirja.

. . . . . .

. . . . . .

. . . . . .

Veebitekstide lugemise oskused ja strateegiad

Kari Kivinen

Demokraatia tugevus sõltub inimeste võimalusest pääseda ligi usaldusväärsele teabele.

Veebikeskkonnad *vs.* veebivälised keskkonnad

Kozyreva jt väidavad oma suurepärases artiklis „Kodanikud *vs*. internet" (1), et veebikeskkonnad on täis nutikaid, väga kohanemisvõimelisi valikusüsteeme, mis on loodud eelkõige ärihuvide maksimeerimiseks, kasutajate tähelepanu püüdmiseks ja hoidmiseks, kasutajate andmetelt raha teenimiseks ning tulevase käitumise prognoosimiseks ja mõjutamiseks. Halvimal juhul võib see hõlbustada desinformatsiooni levikut.

Veebikeskkonnad ja veebivälised keskkonnad erinevad üksteisest ja see mõjutab oluliselt inimeste veebikogemust ja -käitumist. Veebikeskkonnas saab sõnumit edastada miljonitele inimestele, samas kui silmast silma suhtlemisel on füüsilised piirid, kui palju inimesi saab vestlusega liituda (2).

Veebikeskkonnad on sageli loodud ärihuvide maksimeerimiseks, kasutajate tähelepanu püüdmiseks ja hoidmiseks, kasutajate andmetelt raha teenimiseks ning tulevase käitumise prognoosimiseks ja mõjutamiseks.

Digikeskkondades kõigile kättesaadava teabe hulk on üüratu ning mis tahes teavet on võimalik vaevata ja kiiresti jagada suure hulga inimestega. Võrreldes enamiku veebiväliste keskkondadega arenevad veebikeskkonnad kiiresti ja pidevalt: sisu saab kogu aeg muuta, eemaldada ja lisada.

Kozyreva jt tuvastasid nelja tüüpi probleemid, mis on iseloomulikud veebikeskkondadele: suunavad ja manipuleerivad valikusüsteemid, tehisintellekti abil toimivad teabesüsteemid, vale ja eksitav teave ning tähelepanu hajutavad keskkonnad. Kui inimesed kasutavad otsingumootoreid internetist info leidmiseks, mõjutavad nende otsitulemusi algoritmid, mille korporatsioonid on välja töötanud „kasumi saamise eesmärgil ja vähese läbipaistvuse või ametliku järelevalvega". Lisaks, „demokraatlikes riikides on tehnoloogiaettevõtted enda kätte koondanud enneolematuid ressursse, turueeliseid ja kontrolli inimeste andmete ja teabele juurdepääsu üle" (3). Internetikasutajatelt andmete kogumine põhineb kõrgelt arenenud masinõppesüsteemidel ja algoritmidel, mis on meist, inimestest, võimsamad ning ei ole läbipaistvad. Seetõttu on otsimootorite ja näiteks YouTube'i soovitussüsteemi tulemused individuaalsed ja ettearvamatud.

Üks lahendus sellele probleemile on haridus. Teadlaste sõnul õpetaksid avalikkusele kui teabe vastuvõtjale ja loojale suunatud tegevused (näiteks koolide digitaalse infopädevuse õppekavades) õpilastele, kuidas otsida, filtreerida, hinnata ja hallata andmeid, teavet ja digisisu (4). Kõigil neil põhjustel tuleks traditsioonilist lugemisoskust täiendada uut tüüpi veebipõhiste hindamisstrateegiate ja veebitekstide lugemise oskustega.

Tööriistakast veebitekstide lugemiseks

Tuleb märkida, et ainult heast digikirjaoskusest ei piisa. Head aineteadmised aitavad teabe usaldusväärsust paremini hinnata (5). Kui sa mõnda teemat hästi tunned, on sind raskem eksitada. Kliimamuutuste mõistmine on hea näide: kui inimesel on mõne teema kohta head teadmised, siis on teda raskem eksitada (6). Üldine kõrgharidus ei pruugi sind desinformatsioonis orienteerumises siiski kuigi palju osavamaks muuta (7).

Oskus internetist usaldusväärset teavet leida on vajalik, et kogukonnaelus teadlikult osaleda – see on uus kodanikuoskus. See vajadus on eriti terav noorte puhul, kes pöörduvad sageli interneti poole, et sotsiaalsete ja poliitiliste teemade kohta teavet leida. Õpilaste ettevalmistamine veebisisu hindamiseks, eriti kui see puudutab sotsiaalseid ja poliitilisi teemasid, on kooskõlas laiemate pingutustega, mille eesmärk on taasvõimestada kõrgkoole ühiskondlikke ülesandeid täitma. Hiljutise uuringu (8) kohaselt kasutas enamik õpilasi digitaalse info hindamiseks ebatõhusaid strateegiaid. Seetõttu on äärmiselt ajakohane ja oluline edendada veebitekstide lugemise oskusi ja veebipõhiseid hindamisstrateegiaid.

Eelkummutamine

Eelkummutamiseks (ingl *pre-bunking*) nimetatakse protsessi, mille puhul inimesi hoiatatakse ette, et neist on saamas valeinfo sihtmärgid. Eelkummutamise oskusi saab edendada, andes inimestele teatud teema kohta kõigepealt faktilist ja põhjalikku teavet ning tutvustades seejärel sama teema kohta levivat desinformatsiooni. Samuti võib enne teada anda, millist desinfot on oodata.

Mõjus eelkummutamine tegeleb inimeste muredega, räägib nende kogemustest ja suunab neid omaenda asjakohaseid teadmisi jagama. Eelkummutamine on tõhus: selle tegevuse mõte on luua usalduslik suhe oma publikuga, mitte lihtsalt fakte korrigeerida.

Uurimused on näidanud, et loogikapõhine meetod on tõhus. Kui õpetada inimesi ära tundma taktikaid, suudavad nad nende kasutust võrreldes üksikute väidetega sagedamini märgata (9).

Eelkummutamise kolm tüüpi:

1) faktipõhine: konkreetse valeväite või narratiivi parandamine;
2) loogikapõhine: manipuleerimistaktikate selgitamine;
3) allikapõhine: halbade teabeallikate väljatoomine.

Kummutamine

Kummutamine (ingl *debunking*) toimub pärast väärteabe ilmumist. Selle tegevuse eesmärk on parandada valeinfot ja takistada teisi uskumast teavet, mis on tõestatavalt vale. Faktikontrolli strateegiaid saab kasutada väär- ja desinfo kummutamiseks.

Valeinfo parandamine või ümberlükkamine on keeruline, kuna inimesed usuvad tuttavat teavet suurema tõenäosusega isegi siis, kui hiljem selgub, et see teave on vale (tuttavlikkuse nn tagasilöögiefekt).

Uurimused näitavad, et väärinformatsiooni parandamisel on kõige tõhusam esitada põhifaktid enne parandamist vajavat väärinfot. Väärinformatsiooni parandamine ei ole piisav; tuleb ka selgitada, miks info on vale, ja esitada tõene teave või selgitus. Kummutamise käsiraamatus (10) määratletakse neli peamist müütide ümberlükkamise valdkonda:

1. Põhifaktid: rõhuta pigem seda, mis on tõsi, kui seda, mis on vale. Uurimused näitavad, et väärinformatsiooni kummutamisel on kõige parem esitada põhifakt enne kummutamist vajavat väärinformatsiooni.
2. Selged hoiatused.
3. Alternatiivne selgitus: „Kui müüt ümber lükata, tekitab see teadmistesse lünga. Tõhus kummutamine peab selle lünga täitma.” Kui soovid ebaõiget teavet asendada, asenda see konkreetse selgitusega, mis infolünga täidab. Püüa asju selgitada nii lihtsalt ja selgelt kui võimalik: inimeste tähelepanu võib hajuda, kui neile esitatakse sama teavet mitu korda. Vahel võib see tähendada mõne nüansi väljajätmist, kui parandatud teavet esimest korda esitatakse.

4. Graafika: visuaalsed esitlused võivad aidata peamisi fakte selgemalt illustreerida.

Allikateadlikkus

On leitud, et tekstimõistmises mõjutab allikateadlikkus märkimisväärselt õpilaste võimet usaldusväärsust ja teavet hinnata, kusjuures mõju tugevus varieerub väikesest suureni (11). Teadmine, kust leida kvaliteetset teavet ja kas allikas on usaldusväärne, võib olla sama tähtis kui allikakriitilisus, et olla hästi informeeritud kodanik (12). Seetõttu on oluline jagada infot, kust saab usaldusväärset teavet ja keda võib usaldada.

Veebiteabe hindamine

Veebiteabe hindamise (ingl *civic online reasoning*) õpetamine (13) on osutunud keerulisemaks ülesandeks. Stanfordi teadlased (14), (15) pakuvad välja, et kui inimene puutub kokku veebiteabega, peaks ta esitama endale kolm põhiküsimust:

1. Kes on teabe taga?
2. Millised on tõendid?
3. Mida ütlevad teised allikad?

Uuringud, mis keskenduvad veebiteabe hindamist arendavatele õppekavadega seotud tegevustele, on olnud tõhusad inimeste digiallikakriitilisuse ja lateraalse lugemise oskuse arendamisel (16).

On näidatud, et noorte õpetamine, kuidas kognitiivseid strateegiaid ja digivahendeid teabe kontrollimiseks kasutada, mõjutab keskmiselt ka nende võimet teha vahet usaldusväärsel ja eksitaval teabel (17). Eriti suutsid eksitavaid uudiseid kummutada teismelised, kes pärast enesetestimist või õppetööd kasutasid digivahendeid nagu tekstiotsingud või pöördpildiotsing (ingl *reverse image search*).

Kõigi teabeotsijate tähelepanuvõime on piiratud ja otsimootorid leiavad sageli tohutu hulga vasteid. Meil ei ole aega ega energiat kõiki tulemusi analüüsida, et endale olulist teavet leida. Seetõttu on mõistlik keskendada oma piiratud tähelepanu olulisele teabele. Selleks vajame strateegilise eiramise oskust.

Strateegiline eiramine

Võimsaid otsimootoreid kasutades saame mõnikord miljoneid vasteid. Kuidas valida teave, mis on kasulik, tõene ja vastab meie esialgsele teabevajadusele? Selles protsessis vajame kriitilise mõtlemise oskust, et hinnata algoritmide pakutud sisu väärtust ning heita kõrvale ja eirata enamikku vastetest.

Herbert Simon (18) märkis juba 1971. aastal, ammu enne internetiajastut, et teabe üleküllus põhjustab tähelepanu nappust. Reklaamijad, korporatsioonid, lobistid, klõpsusöödalehed, vandenõuteoreetikud, vihkamist õhutavad rühmitused ja propagandistlikud valitsused töötavad täie hooga, et internetis meie tähelepanu endale saada. Sellises olukorras on tähelepanu hoidmiseks sageli kõige mõistlikum kasutada strateegilist eiramist. Piiratud tähelepanu tingimustes (19) on tähtsaim otsustada, millele oma tähelepanu suunata.

Seega peame arendama oma oskust eirata suurtes kogustes ebaolulist teavet. Peaksime kasutama strateegilist eiramist, et vältida desinformatsiooni ja pöörata oma piiratud tähelepanu sisule, mis on tõesti lugemist väärt.

Kõrvutav lugemine

Lugeja kontrollib enne teksti lugemist veebiteabe tausta (autori usaldusväärsus, faktid, statistika, allikad jne) eri saitidelt ja allikatest.

Uus vahend digitaalse infopädevuse tööriistakastis on kõrvutav lugemine (ingl *lateral reading*): lugeja kontrollib enne teksti lugemist veebiteabe tausta (allika usaldusväärsus, faktid, statistika, allikad) eri saitidelt ja allikatest.

Kuna veebi- ja võrguväline teabekeskkond on erinevad, tuleb veebiteabe allikale rohkem tähelepanu pöörata. Traditsiooniline lugemisviis ei pruugi digitaalses keskkonnas tõhus olla. Kui oleme tundmatu veebiteabe analüüsimiseks liiga hõivatud ja isegi ei kontrolli, kust artikkel pärineb, siis ei pruugi me märgata, et kogu tekst põhineb kallutatud teabel.

Wineburg ja McGrew (19) vaatlesid, kuidas õpilased, teadlased ja faktikontrollijad senitundmatu võrguteabega tegelevad. Faktikontrollijad avasid oma veebilehitseja horisontaalteljel mitu vahekaarti ja otsisid teavet teksti taga oleva organisatsiooni või isiku kohta. Alles pärast seda, kui nad olid kontrollinud, mida teistel saitidel öeldakse, pöördusid nad teksti juurde tagasi. Niisugust meetodit kasutades suutsid faktikontrollijad kiiresti leida saidid, mis varjasid oma eesmärke ja sponsoreid. Samas eksperimendis keskendusid õpilased ja teadlased algsele saidile; lõpptulemusena jäi segaseks, mis on selle tegelik eesmärk või kes seda rahastab.

Strateegia, mida professionaalsed faktikontrollijad kasutavad veebivoogude lateraalseks lugemiseks mitme ühendatud saidi kaudu konkreetsesse teksti süvenemise asemel, on osutunud kiireks ja tõhusaks viisiks vältida tähelepanu, aja ja energia kulutamist kallutatud teabele. Soovitatav on kasutada klõpsude piiramise strateegiat: enne kui klõpsata otsingutulemustes toodud linkidele, tuleks lehte tähelepanelikult edasi kerida ning otsida tulemusi, mis on asjakohased (ja mis ei pruugi olla esimeste tulemuste seas) ning valida usaldusväärsed teabeallikad (14). Mitme asjakohase allika lugemine, et saaksime teavet kinnitada ja kontekstuaalselt seostada, võimaldab meil allika usaldusväärsuse kohta teadlikke otsuseid teha.

Veebiliikluse reeglid

2022. aasta juulis võttis Euroopa Parlament vastu digiteenuste määruse (20) ja digiturgude määruse (21). Need Euroopa Liidu (EL) uued digieeskirjad kehtestavad enneolematud standardid veebiettevõtete aruandekohustusele avatud ja konkurentsitihedal digiturul. Pärast uute eeskirjade rakendamist on ELi internetikasutajatel rohkem valikuvõimalusi ja nende õigused on internetis paremini kaitstud.

Oleks hea, kui suured veebiplatvormid hakkaksid tulevikus oma sisu hoolikamalt reguleerima, nagu nimetatud määrused ette näevad. Paraku ei saa me platvormide heale tahtele loota. Peame parandama oma digioskusi ja haridust! Kodanikke tuleks õpetada oma kriitilist mõtlemist ja digitaalset infopädevust arendama.

Lihtsad veebiliiklusreeglid oleksid meile kõigile kasulikud. Kui ma koolis käisin, õpetati mulle lihtsaid liiklusreegleid: enne tänava ületamist vaata kõigepealt vasakule, siis paremale ja uuesti vasakule. Vajame samasuguseid selgeid juhiseid ka veebikeskkondadele.

Tundmatu veebisisuga kokku puutudes on alati kasulik vastata neile kolmele lihtsale põhiküsimusele, enne kui kulutada aega sisu lähemalt uurimiseks:

- **Kes on teabe taga ehk allikas?**
- **Millised on tõendid?**
- **Mida ütlevad teised allikad?**

Mõistlik oleks oma piiratud tähelepanu suunata lugemist väärivatele tekstidele!

Viited

(1) Kozyreva, A., Lewandowsky, S., & Hertwig, R. (2020). Citizens Versus the Internet: Confronting Digital Challenges With Cognitive Tools. Association for Psychological Science. SAGE.

(2) Barasch, A., & Berger, J. (2014). Broadcasting and narrowcasting: How audience size affects what people share. Journal of Marketing Research, 51, 286–299. https://doi.org/10.1509/jmr.13.0238

(3) Zuboff, S. (2019). The age of surveillance capitalism: The fight for the future at the new frontier of power. Profile Book.

(4) Breakstone, J., McGrew, S., Smith, M., Ortega, T., & Wineburg, S. (2018). Teaching students to navigate the online landscape. Social Education, 82, 219–221.

(5) Lurie, E., & Mustafaraj, E. (2018, May). Investigating the Effects of Google's Search Engine Result Page in Evaluating the Credibility of Online News Sources. In Proceedings of the 10th ACM Conference on Web Science (lk 107–116).

(6) Nygren, T., & Guath, M. (2021). Students evaluating and corroborating digital news. Scandinavian Journal of Educational Research, in press.

(7) Roozenbeek, J., van der Linden, S., & Nygren, T. (2020). Prebunking interventions based on „inoculation" theory can reduce susceptibility to misinformation across cultures. Harvard Kennedy School Misinformation Review, 1(2).

(8) Breakstone, J., Smith, M., Ziv, N., & Wineburg, S. (2022). Civic Preparation for the Digital Age: How College Students Evaluate Online Sources about Social and Political Issues, The Journal of Higher Education. https://doi.org/10.1080/00221546.2022.2082783

(9) First Draft. https://firstdraftnews.org/articles/a-guide-to-prebunking-a-promising-way-to-inoculate-against-misinformation/

(10) Debunking Handbook (2020). https://www.climatechangecommunication.org/wp-content/uploads/2020/10/DebunkingHandbook2020.pdf

(11) Brante, E. W., & Strømsø, H. I. (2018). Sourcing in Text Comprehension: a Review of Interventions Targeting Sourcing Skills. Educational Psychology Review, 30(3), 773–799. doi:10.1007/s10648-017-9421-7

(12) Haider, J., & Sundin, O. (2020). Information literacy challenges in digital culture: conflicting engagements of trust and doubt. Information, Communication & Society, 1–16. doi:10.1080/1369118X.2020.1851389

(13) Civic Online Reasoning site of Stanford University. https://cor.stanford.edu/

(14) Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., & Saavedra, A. (2021). Students' Civic Online Reasoning: A National Portrait. Educational researcher, 50(8), 505–515. doi:10.3102/0013189X211017495

(15) Wineburg, S., Breakstone, J., McGrew, S., Smith, M., and Ortega, T. (2022). Lateral Reading on the Open Internet: A District-Wide Field Study in High School Government Classes. Journal of Educational Psychology (Accepted for publication).

(16) McGrew, S., & Byrne, V. L. (2020). Who Is behind this? Preparing high school students to evaluate online content. Journal of Research on Technology in Education, 1–19. doi:10.1080/15391523.2020.1795956

(17) Axelsson, C.-A. W., Guath, M., & Nygren, T. (2021). Learning How to Separate Fake From Real News: Scalable Digital Tutorials Promoting Students' Civic Online Reasoning. Future Internet, 13(3), 60, 1–18.

(18) Simon, H. A. (1971). Designing organizations for an information-rich world. M. Greenberger (toim.), Computers, communications, and the public interest (lk 37–72). John Hopkins University Press.

(19) Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. Teachers College Record, 121(11), Article 22806. https://www.tcrecord.org/content.asp?contentid=22806

(20) DSA. https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment

(21) DMA. https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users

Ülesanded

1. Mille poolest erinevad veebikeskkonnad ja veebivälised keskkonnad?

2. Millised on sinu harjumused veebis? Keda sa jälgid, mida kuulad ja loed?

3. Palun tee faktikontroll järgmisele uudisele (skaneeri QR-kood). 

4. Kuidas internetis suurt hulka ebaolulist teavet eirata?

Seisa oma õiguste eest! Veebikeskkonnad: kasutajatest kodanikeks

Minna Aslama Horowitz

Sotsiaalmeedia kasutajatena tahame saada teavet ja veel sagedamini meelelahutust. Meile meeldivad näiliselt vaba juurdepääs, funktsioonid ja piirideta ühenduvus. Võime isegi teada hinda, mida oma andmeid loovutades maksame – ning mõned meist võivad öelda, et see on mõistlik kogu selle sisu ja lõbusate funktsioonide eest, mida nad meile pakuvad just nii, nagu meile meeldib. Paraku mõtleme harvem platvormidest kui võimsatest avalikest areenidest, mis võivad mõjutada meie vaimset tervist, kutsuda üles vägivallale mõne ühiskonnagrupi vastu, mõjutada valimistulemusi või õhutada sõdu.

Digiajastu on toonud digiplatvormid üksikisikute õigusi käsitlevate ülemaailmsete aluspõhimõtete toetamise või rikkumise keskmesse. Sellest vaatenurgast oleme kodanikud. Meie tegevusega kaasneb vastutus ja see on seotud ka põhiliste inimõigustega. Senini ei ole olemas ühtegi õigusnormi meie kui digitaalsete maailmakodanike õiguste kohta, kuid paljud huvirühmad on kaasatud aruteludesse, kuidas neid õigusi määratleda ja kaitsta. Selles peatükis kirjeldatakse, kuidas digiplatvormid, ÜRO, Euroopa Liit ja kodanikuühiskond meie digitaalõigusi mõistavad ja kaitsevad.

Inimõigused digiajastul

Tänapäeval mõjutavad platvormid ja muud tehnoloogiaettevõtted nii suurt osa meie elust ja ühiskonnast, et neil on ülisuur roll ka meie põhiõiguste kasutamise võimaldamisel või piiramisel. Internetiühendus avab meile värava piiramatu sisu juurde, kuid platvormid on ka Google'i või TikToki soovitatud teabe n-ö

valvurid. Saame oma andmete eest tasuta teenuseid, kuid sageli me ei tea, kuidas neid andmeid kasutatakse ja kuidas see meie privaatsust mõjutab. Saame end kergesti ja vabalt väljendada, kuid samal ajal puutume kokku ka ohtra valeinformatsiooni, manipulatsiooni ja vaenu õhutamisega. Nagu ÜRO peasekretäri digikoostöö aruandes märgitakse, ei aita digitehnoloogia mitte ainult õigusi propageerida, kaitsta ja teostada, vaid seda kasutatakse ka inimõiguste mahasurumiseks, piiramiseks ja rikkumiseks (1).

Küsimus ei ole ainult sõjatsensuuris või interneti väljalülitamises, mis võib toimuda kaugel meie igapäevaelust. Tegelikult teame vähe sellest, kuidas meie kui globaalsete digiplatvormide kasutajate õigusi kaitstakse. Organisatsioon Ranking Digital Rights jälgib, mida suured platvormid ja telekommunikatsiooniettevõtted üle maailma meile meie õiguste kohta teada annavad. Nende koostatav Big Tech Scorecard reastab ettevõtteid selle järgi, kuidas nad meile oma sise-

eeskirjadest ja tavadest (juhtimisest) teada annavad, kuidas nad meie privaatsust käsitlevad ning kuidas meie sõnavabadust kaitsevad. Kahjuks hoiavad need hiiglased alates Amazonist ja Alibabast kuni X-i ja Yandexini meid pimeduses. Kui keegi ka leiab teavet nende teenusetingimuste ja kasutajate õiguste kohta, võivad need olla raskesti arusaadavad ning sageli puudub neis oluline teave, näiteks kellega nad meie andmeid jagavad või kas nad järgivad oma algoritmide arendamisel rahvusvahelisi inimõigusi. Ja isegi kui sellisel ettevõttel nagu Meta on inimõiguste kaitse põhimõtted, on üksikisikutel või sõltumatutel organisatsioonidel praktiliselt võimatu nende rakendamist jälgida (2).

Kuidas ÜRO ja EL meie õigusi käsitlevad

ÜRO on aasta-aastalt üha enam mures digitaliseerimise mõju pärast meie maailmas. Paljud probleemid, millega me digiajastul silmitsi seisame, on juba kantud kõige tuntumasse ja globaalsemasse meie õigusi käsitlevasse juhendisse: ÜRO 1948. aasta inimõiguste ülddeklaratsiooni (3). Näiteks artiklis 12 on sätestatud õigus privaatsusele ja artiklis 19 käsitletakse sõnavabadust.

ÜRO püüab inimõiguste ja kommunikatsiooni teemadega tegeleda üldisemalt oma inimõiguste nõukogu (4) ja inimõiguste ülemvoliniku büroo (5) kaudu ning konkreetsemalt oma interneti haldamise foorumi (6) kaudu – see on riikide, ettevõtete, teadlaste ja kodanikuühiskonna esindajate iga-aastane kohtumine. Kuna eraettevõtete kätte (Google'ist TikTokini) on kogunenud suur võim, kasutatakse ka ÜRO äritegevuse ja inimõiguste juhtpõhimõtteid (7), et rõhutada tehnoloogiaettevõtete õigustepõhiseid kohustusi. Kuigi ÜRO ei koosta seadusi, võtab ta seisukoha sellistes küsimustes nagu digitaalne ühenduvus kui inimõigus (8) või tehisintellekti eetilised suunised (9).

Veel üks oluline ja teedrajav osaline meie digitaalõiguste määratlemisel on Euroopa Liit (EL). Oma põhjaliku kavaga Euroopa digitaliseerimiseks aastaks 2030, mida tuntakse digikompassi nime all (10), ei loo EL seadusi mitte ainult oma digimajanduse toetamiseks, vaid ka digiturvalisuse tagamiseks ja oma kodanikele rohkemate võimaluste andmiseks. Kompassi aluspõhimõtted on sätestatud Euroopa demokraatia tegevuskavas ning need hõlmavad ka kodanike õiguste ja osaluse olulist rolli ning desinformatsiooniga võitlemist (11). 2022. aastal tegi EL ettepaneku võtta vastu Euroopa deklaratsioon digiõiguste ja -põhimõtete kohta. See on esimene rahvusvahelise valitsusorganisatsiooni kodanikukeskne ja õigustel põhinev deklaratsioon. Deklaratsioonis rõhutatakse kaasamist, osalemist, kasutajate valikuid, turvalisust ja jätkusuutlikkust digikeskkonnas (12).

Natukese abiga...

Lõppude lõpuks on meie õigused meie endi teha. Praegu puudub digipõhiseadus, mis meie õigused kogu maailmas kinnitaks. Tehnoloogia areneb nii kiiresti, et igasugused detailsed õigused võivad vananeda kohe pärast nende kehtestamist.

Digikeskkond võib meid valgustada, lõbustada ja harida. See võib aidata meil olla uuenduslikud, tegelda loominguga, elatist teenida, suhelda ja midagi paremaks muuta. Selle tohutu positiivsete muutuste potentsiaali tõttu peaksime digikodanikena oma õigusi ja nendega seotud kohustusi tõsiselt võtma. Saame seda teha mitmel rindel.

- ÜRO määrab kindlaks aluspõhimõtted ja rahvusvahelised foorumid meie õiguste üle arutlemiseks.
- EL pakub toetust mitmesuguste seadusandlike algatustega, peamiselt hiljutise digiteenuste määruse paketiga, mille eesmärk on reguleerida eelkõige suurimate ülemaailmsete platvormide tegevust (13).
- Kodanikuühiskonna organisatsioonid ja rühmad, kes on sageli teerajajad digikahjude ja -probleemide käsitlemisel, saavad meid kursis hoida digitaalõiguste eri aspektide arenguga.
- DigComp 2.2 abil annab EL meile ka raamistiku, mis aitab mõista, milliseid digitaalseid kodanikuoskusi me vajame: teadmisi digitaalsest infopädevusest, võimalusi suhelda, teha koostööd ja luua sisu ning lahendada probleeme digikeskkonnas, samuti ka võimet kaitsta oma privaatsust.

Viited

(1) Report of the Secretary-General Roadmap for Digital Cooperation
https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

(2) Key Findings from the 2022 RDR Big Tech Scorecard https://rankingdigitalrights.org/mini-report/key-findings-2022/

(3) Universal Declaration of Human Rights https://www.un.org/en/about-us/universal-declaration-of-human-rights

(4) United Nations Human Rights Council https://www.ohchr.org/en/hr-bodies/hrc/about-council

(5) United Nations Human Rights. Office of the High Commissioner https://www.ohchr.org/en/ohchr_homepage

(6) Internet Governance Forum https://www.intgovforum.org/en

(7) Guiding Principles on Business and Human Rights: Implementing the United Nations
"Protect, Respect and Remedy" Framework
https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights

(8) The Case for Connectivity, the New Human Right
https://www.un.org/en/un-chronicle/case-connectivity-new-human-right

(9) Ethics of Artificial Intelligence https://en.unesco.org/artificial-intelligence/ethics

(10) Europe's Digital Decade: digital targets for 2030 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

(11) European Democracy Action Plan: Making EU democracies stronger
https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

(12) European Declaration on Digital Rights and Principles for the Digital Decade
https://ec.europa.eu/newsroom/dae/redirection/document/82703

(13) The Digital Services Act package
https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

Ülesanded

1. Mis on tehnoloogia kasutamise plussid ja miinused? Palun nimeta mõned neist.

2. Mida mõtleb artikli autor, kui ta ütleb, et tehnoloogiahiiud hoiavad meid pimeduses?

3. Ava oma telefoni seaded, otsi üles rakendus, mida kasutad kõige rohkem, ja kontrolli, millised õigused oled sellele andnud. Kas on midagi, mida sooviksid selles osas muuta?

Räägime infohäiretest

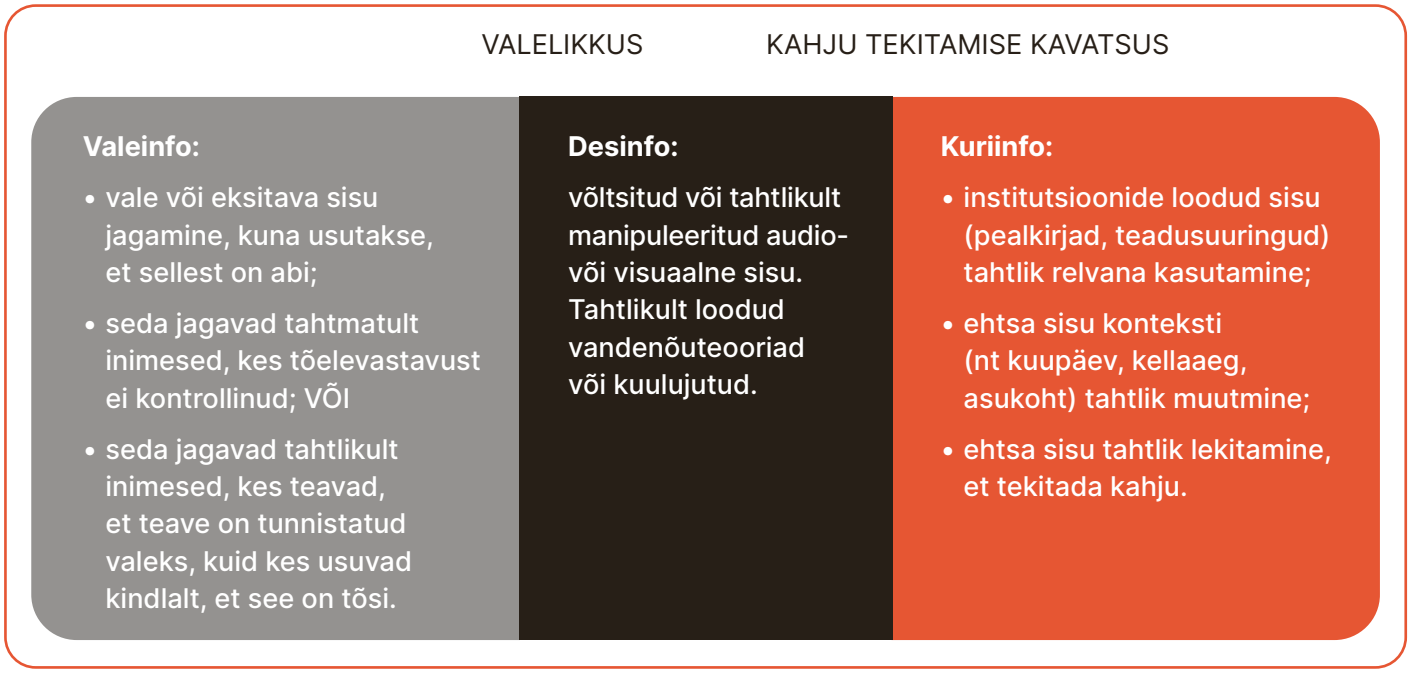
Minna Aslama Horowitz

Võltsuudised! Propaganda! Manipuleerimine! Vandenõu! Digimaailmas levib katkuna sisu, mis on kogemata või tahtlikult vale, kahjulik või mõlemat. Selles peatükis käsitletakse, kuidas teha algust haiguste ja nende sümptomite mõistmisega, et toetada meie digitervist.

Kitsas lähenemine infohäiretele keskendub teabele, mis on tõendatavalt vale. Seda vormi on suhteliselt lihtne tuvastada ja selle vastu saab võidelda faktikontrollijate palkamisega, kahtlaste postituste märgistamisega, valeuudiste eemaldamisega jne. Raskemini diagnoositavad on tahtlikud katsed moonutada uudiseid, et levitada ideoloogiaid, ajada segadusse, tekitada lõhestumist ja levitada desinformatsiooni raha teenimise eesmärgil. Kuigi paljud nendest tegevustest võivad olla poliitiliselt motiveeritud, võivad need katsed esineda ka klõpsusöödа ja uudiste tahtliku filtreerimise vormis, et kindlaid inimesi ligi meelitada.

Et aidata meil mõista internetis esineva valesisu mõõtmeid, koostasid Claire Wardle ja Hossein Derakhshan (1) infohäirete skeemi. Sellel eristatakse eri liiki sisu kasutuseesmärgi põhjal:

- valeinfo – vale seos või eksitav sisu, mis võib olla ka tahtmatu ja mis ei ole alati kahjulik. See hõlmab ka jagatud sisu, mida peetakse tõeseks ja mis seetõttu tuleks avalikustada üldsuse huvides, isegi kui selle tõelevastavust ei ole kontrollitud;



Joonis. Infohäirete liigid

- desinfo – tahtlikult vale kontekst, sealhulgas tahtlikult loodud vandenõuteooriad või muu sisu, mis võib mõnel juhul olla kahjulik, ning
- kuriinfo – vale sisu, mis on loodud tahtlikult kahju tekitamiseks või sisu kasutamine pahatahtlikel eesmärkidel.

Tavainimestele ei pruugi häirete liikide eristamine alati selge olla, kuid neil, kes püüavad häireid eemaldada, on oluline sellest aru saada. Ajakirjanikud, poliitikakujundajad ja teadlased kasutavad infohäirete skeemi sageli kui abivahendit internetis leiduva valesisu käsitlemisel. Loomulikult peavad nad keskenduma tõeliselt kahjulikule sisule. Õiguslikust seisukohast on olulised kaks küsimust: millised on sisu looja kavatsused ja sisu ise ning kui ebatõene see on. Ajakirjanik võib kogemata lisada uudisesse ebatäpset teavet, seevastu propagandist võib teadlikult luua täielikult fabritseeritud sisu, mille eesmärk on inimesi petta (2).

Tegelikkuses võib infohäire esineda eri vormides. Näiteks on Euroopa Liidu eri huvirühmi hõlmav kõrgetasemeline valeuudiste ja veebis leviva desinformatsiooni eksperdirühm tuvastanud probleemse tegevuse, mis on palju ulatuslikum kui ükskõik millised nn uudised: automatiseeritud kontod, võltsjälgijate võrgustikud, fabritseeritud või manipuleeritud videod, sihitud reklaam, organiseeritud trollimine, visuaalsed meemid jne.

Infohäire hõlmab ka mitut liiki tegevusi. Peale võltssisu loomise levitatakse desinfot mitmel viisil, sealhulgas postitades, kommenteerides, jagades, säutsudes ja säutse jagades.

Kokkuvõttes ei ole infohäire põhjuseta, „niisama kuidagi" tekkinud haigus, vaid eri huvirühmade tegevus, mis aitab veebikahjusid kas tekitada või kõrvaldada. Veebiplatvormid ja nende aluseks olevad võrgud, protokollid ja algoritmid muudavad väär-, des- ja kuriinfo levitamise lihtsaks ja kontrollimatuks. Kuna globaalsed platvormid teenivad kasutajate andmetelt raha, ei ole valeinfo leviku piiramine nende huvides, kui see info toob neile vaatamisi, meeldimisi ja jagamisi. Samuti võivad mitmesugused riiklikud või mitteriiklikud poliitikategijad, kasumitaotlejad, kodanikud individuaalselt või rühmadena ning info levitamise ja võimendamise taristud (sealhulgas uudismeedia) soovida valeteabe levikut kas peatada või hoopiski seda luua ja laiemalt levitada (3).

Viited

(1) Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making. Euroopa Nõukogu.
https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

(2) Nt Möller, J., Hameleers, M., & Ferreau, F. Types of disinformation and misinformation.
Various types of disinformation and their dissemination from a communication science and legal perspective.
https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Publikationen/Weitere_Veroeffentlichungen/GVK_Sum

(3) Vt Final report of the High Level Expert Group on Fake News and Online Disinformation.
https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation

Ülesanded

1. Mille poolest erinevad vale-, des- ja kuriinfo?
   Palun ühenda omadussõnad vale-, des- või kuriinfo mõistega.

   vale, eksitav, kahju tekitamiseks mõeldud, tahtlikult vale, vaenulik, poliitiline, luureagentuuri levitatud, lõhestav, tahtlik, ekslik, kontekstist välja rebitud, laimamiseks mõeldud, vigaselt kirjutatud

2. Palun too veel mõned näited infohäirete kohta nagu võltskontode loomine, vihaste kommentaaride kirjutamine.

3. Pane artiklile „Kuulmine teravneb kõndides” eksitav pealkiri.

Kuulmine teravneb kõndides

Priit Ennet

Koerad, kassid, põdrad, hobused — paljud loomad oskavad nii toredasti kõrvu liigutada, suunata kõrvalestad just sesse suunda, kust huvipakkuv heli lähtub.

Inimeste eellased on selle oskuse minetanud juba umbes 25 miljonit aastat tagasi, selle asemel hoolitseb inimesel aga kuulamise suundteravustamise eest aju ise.

Saksa ja Hiina teadlased eesotsas Barbara Haendeliga Würzburgi Ülikoolist mõõtsid ette mängitud helisid kuulvate inimeste aju elektrilaineid. Mõõteaparaadiks võtsid nad uuendusliku elektroentsefalograafi, mis võimaldas katseisikutel ajumõõtmise ajal ruumis vabalt ringi liikuda, sest neile pähe pandud elektroodid saatsid andmeid põhiseadmesse traadita. Sedalaadi seadmed on viimasel ajal üldse hakanud ilmsiks tooma, kui tähtis on tegelikult üldse inimese ajutegevusele liikumine.

Haendeli uurimisrühm on ka ise varem avastanud, et kõndiv inimene märkab nägemisvälja perifeerias asju, mida ta paigal seistes ei pane tähele. Nüüdses katses paluti 35 katseisikul kõndida mööda number 8 kujulist rada, elektroodid peas ja liikumisandurid küljes, kuulates samal ajal pidevat häältevoogu. Selgus, et kui katseisik hakkas liikuma, siis aktiveerus ta ajus häälelise teabe töötlemine selgelt võrreldes paigaloleku ja isegi paigalkõnniga. Kui katseisik oma rajal pööras, siis hakkas aju pöörama teravamat tähelepanu uuelt liikumissuunalt tulevale helile. Rajal kulgemise ajal pendeldas kuulmistähelepanu seega pidevalt vasakule-paremale.

Teadlased kirjutavad ajakirjas The Journal of Neuroscience, et niisugune tähelepanu suunamise võime on aidanud inimesel ja ta eellastel oma looduslikus helikeskkonnas paremini toime tulla. Avastus aitab ka aru saada, miks tunduvad liikumisharjutused olevat aju tervisele kasulikumad kui seisuharjutused — meeled teravduvad, vaim virgub; vaimu-tervise juured on liikumises.

Ilmunud: ERR Novaator
https://novaator.err.ee/1609825872/kuulmine-teravneb-kondides

Psühholoogilisel manipulatsioonil põhinev poliitiline propaganda

Joonas Pörsti

Poliitiline propaganda on laiaulatuslik mõjutusvorm, mille eesmärk on veenda sihtrühma tegutsema propagandisti eesmärkide kohaselt. Propaganda tunnusjoon on psühholoogiline manipuleerimine, tavaliselt desinfo ehk eksitava teabe tahtliku levitamise kaudu. Vahendite valik ei piirdu aga ainult desinformatsiooniga. Seda võib kasutada ka kuriinfo levitamiseks, st tõese teabe levitamiseks eesmärgiga kedagi diskrediteerida või muul viisil kahjustada. Tõhus propaganda tugineb ka osalisele tõele, algsest kontekstist välja võetud sisule ja teabe varjamisele (1).

Propaganda keskmes on tavaliselt alternatiivne, mustvalge, lihtsustatud narratiiv, mis filosoof Hannah Arendti (2) sõnul „vastab inimmõistuse vajadustele paremini kui tegelikkus". Osav propagandist kohandab oma meetodeid publiku ootuste järgi selliselt, et nad ei saaks aru, et neid on petetud. Inimesed kalduvad omaks võtma propagandat, mis tugevdab nende sotsiaalset staatust ja identiteeti, vähemalt vaimsel tasandil.

Propaganda ei piirdu ainult teabe levitamisega, vaid käib käsikäes sihtrühma manipuleerimisega mitmesuguste ettevõtmiste kaudu: kohtuasjad, lavastatud või n-ö ülevalt alla suunatud ühiskondlikud liikumised ja massiüritused, vägivallaaktid, ahistamine või sõjalised ähvardused. Propaganda on demokraatlikele ideaalidele kahjulik, kuna selle eesmärk on piirata avalikku arutelu poliitiliste valikute üle ilma ratsionaalse põhjenduseta (3). Propagandist võib sellest hoolimata esineda sõnavabaduse ja demokraatia kaitsjana. Neid väärtusi kasutatakse sageli sümboolsete loosungitena, kuigi tegelik eesmärk on demokraatlikke institutsioone õõnestada.

Algselt tähendas propaganda lihtsalt õige õpetuse levitamist. Mõiste sündis 1622. aastal, kui paavst Gregorius XV asutas Roomas „püha kogukonna usu levitamiseks", Sacra Congregatio de Propaganda Fide, et teenida reformatsiooni ja teha katoliku misjonitööd. Mõiste omandas negatiivse tähenduse alles pärast 20. sajandi maailmasõdu (4). Eriti demokraatlikes ühiskondades on propaganda sellest ajast alates seostunud autoritaarsete ühiskondadega nagu Natsi-Saksamaa, Nõukogude Liit, Hiina või Vladimir Putini Venemaa.

Kuid propagandat levitatakse ka demokraatlikes ühiskondades ja sõnavabadus võib need ühiskonnad propagandistliku mõju suhtes eriti haavatavaks muuta. Viimastel aastatel on propaganda süstemaatiline kasutamine Ameerika Ühendriikides lõhestanud poliitilist õhkkonda ja muutnud sotsiaalsed reformid keerulisemaks. Pärast 2020. aasta presidendivalimiste kaotamist destabiliseeris Donald Trump riigi poliitilist süsteemi, levitades narratiivi „varastatud valimistest". Propagandakampaania kulmineerus 6. jaanuaril 2021, kui Trumpi toetajad ründasid USA Kongressi ja üle saja politseiniku sai Washingtonis Capitol Hillil vigastada (5). Samamoodi on Ungari president Viktor Orbán kasutanud propagandat poliitilise opositsiooni vaigistamiseks ja demokraatlike institutsioonide õõnestamiseks.

Riiklik propaganda on olnud peamine võimu teostamise vorm ka Vladimir Putini ajal Venemaal. Putin sai presidendiks 2000. aastal demokraatlikel valimistel, kuid Venemaa presidendi administratsioon oli juba valmis kasutama propagandat oma sise- ja välispoliitiliste eesmärkide saavutamiseks. Riigi poliitiline opositsioon suruti maha ja kriitilised hääled vaigistati, koondades telekanalite omandiõiguse võimulolijate kätte. Presidendi positsiooni tugevdas ka juhikultuse loomine. Samal ajal maksimeeris Putini režiim oma välispoliitilist manööverdamisruumi, jätkates Venemaal näiliselt demokraatlike väärtuste järgimist (6).

Propaganda on suure hulga inimeste mobiliseerimine poliitilistel eesmärkidel, kuid see ei piirdu ainult valitsustega – seda võivad levitada erakonnad, ideoloogilised rühmitused, ettevõtete palgatud lobistid või sotsiaalmeedias organiseerunud kodanikuaktivistid. Propaganda üldiselt ei suuda inimeste meelsust järsult muuta, kuid võib järk-järgult hoiakuid soovitud suunas nihutada. Kõige tõhusam ja kiirem viis on siiski kasutada ära olemasolevaid eelarvamusi, st sügavalt juurdunud uskumusi ja väidetavaid vaenlasi. Psühholoogiline manipuleerimine põhineb sihtmärkide eelarvamuste heal tundmisel. Propagandat saab kujundada kultuuriteadmiste, sotsioloogiliste uuringute ja arvamusküsitluste põhjal. Ajalooliselt väljakujunenud kultuurimüüdid on eriti kasulikud, kuna kujundavad maailmavaadet ja pakuvad seega propagandale valmis raamistikku. Müüdid suunavad inimeste sotsiaalset kujutlusvõimet ning on seotud arusaamadega sellest, mis on püha: rahvus, selle päritolu ja traditsioonilised väärtused (7).

Näited sellistest müütidest on Natsi-Saksamaa antisemiitlik ideoloogia, narratiiv Venemaast kui „kolmandast Roomast", mis kaitseb kristlust, või USAst kui maailma vabaduse kaitsjast. Propaganda on üles ehitatud vastasseisudele: Natsi-Saksamaal rajati militaristliku kangelase kuju „madalamatele rassidele" ja juutidele, kes sildistati kui erilised süntüübid (8).

21. sajandil on internet ja eriti sotsiaalmeedia pakkunud uusi vahendeid propaganda levitamiseks. Emotsionaalsed sõnumid levivad sotsiaalmeediavõrgustikes kiiresti, seal puuduvad traditsioonilise meedia valvurid ja sõnumi päritolu võib olla varjatud anonüümsete kontode taha. Sotsiaalmeedias on lihtne levitada nn musta propagandat, kus manipuleerivaid sõnumeid saadetakse vastaspoole identiteedi alt. Näiteks võib selleks luua ühe teemaga seotud liikumise või uudistelehe. Sisu piirab ainult kujutlusvõime: propaganda eesmärk võib olla sotsiaalsete pingete suurendamine või avalikkuse eksitamine ebaoluliste või moonutatud teemadega. Nn musta propaganda sisu võib olla täielikult võltsitud või osaliselt tõene. Sõnumi tegelik allikas püüab jääda varjatuks, et propaganda ei pöörduks tema enda vastu.

Algusaegadel ei olnud digiteenused reguleeritud ja näiteks ISIS sai vabalt levitada oma vägivalda õhutavat propagandat Facebookis, X-is ja YouTube'is (9). Praeguseks on digiplatvormid hakanud oma sisu rohkem reguleerima, kuid nende ärikasumi loogika suunab külastajad ikka veel lõhestava ja emotsionaalse sisu juurde, mis pakub rohkelt vahendeid propagandaks. Propaganda kattub kogu muu kommunikatsiooni, turunduse ja uudistega ning veebis on need kõik koos (10). Ka faktikontroll on suurenenud, kuid digiplatvormide teabealaste mõõdalaskmistega ei tulda ikka veel toime.

Internetiajastul on näiteks Venemaa kasutanud oma propagandas mudelit, mida USAs asuv Rand Institute on nimetanud valede vooluks (11). Selle mudeli puhul esitab propagandist sündmustest kiiresti erinevaid segadusttekitavaid versioone, pööramata erilist tähelepanu nende usaldusväärsusele. Strateegia eesmärk on õõnestada meedia ja demokraatlikult valitud otsustajate usaldust „alternatiivsete tõdede" ja vandenõuteooriate abil (12). USA radikaalsed parempoolsed on kasutanud samasuguseid meetodeid. Kui enam ei olegi olemas tõde või midagi, mida peetakse tõeseks, on propagandistil vabamad käed oma poliitikat ellu viia. Digitaalne infopädevus ja propagandatehnikate mõistmine on sellise propaganda vastumürk. Propaganda mõju saab nõrgestada, kui selle meetodid avalikustatakse, kuna see vähendab manipulatsiooni tõhusust ja võimaldab avalikkusel propagandistlikke sõnumeid eirata (13).

Viited

(1) Jowett, Garth, & Victoria O'Donnell (1992). Propaganda and Persuasion. Los Angeles: Sage.

(2) Arendt, Hannah (1958). The Origins of Totalitarianism. Cleveland: George Allen & Unwin.

(3) Stanley, Jason (2015). How Propaganda Works. Princeton: Princeton University Press.

(4) Taylor, Philip M. (2003). Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era. Manchester: Manchester University Press.

(5) Hasen, Richard (2022). Cheap Speech. How Disinformation Poisons Our Politics — and How to Cure It. New Haven: Yale University Press.

(6) Dawisha, Karen (2014) Putin's Kleptocracy; Who Owns Russia? New York: Simon & Schuster.

(7) Ellul, Jacques (1973). Propaganda: The Formation of men's attitudes. New York: Vintage Books.

(8) Klemperer, Victor (2002). The Language of the Third Reich. London & New York: Continuum.

(9) Berger, Jessica, & J. M. Stern (2016). Isis: The State of Terror. London: HarperCollins.

(10) Valaskivi, Katja (2018). Beyond Fake News: Content confusion and understanding the dynamics of the contemporary media environment. Helsingi: Hybrid CoE, veebruar. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-5-beyond-fake-news-content-confusion-and-understanding-the-dynamics-of-the-contemporary-media-environment/

(11) Paul, Christopher, & Miriam Matthews (2016). The Russian „Firehose of Falsehood" Propaganda Model. Santa Monica: Rand.

(12) Lucas, Edward, & Peter Pomerantsev (2016). Winning the Information War: Techniques and Counter Strategies to Russian Propaganda in Central and Eastern Europe. Washington: Center for Eastern European Policy.

(13) Nimmo, Ben (2015). Anatomy of an Info-War: How Russia's Propaganda Machine Works and How to Counter It. Central European Policy Institute. https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/

Ülesanded

1. Täida lüngad:

   Propaganda on ....., eriti kallutatud või ..... iseloomuga, mida kasutatakse poliitiliste eesmärkide või seisukohtade edendamiseks.

   Propaganda on teabe – faktide, ..., kuulujuttude, ... või valede – ..... mõjutamiseks.

   Propagandistidel on kindel ..... või eesmärkide kogum.

2. Millistes eluvaldkondades saab propagandat rakendada?

. . . . . .

. . . . . .

. . . . . .

3. Palun too mõned näited propagandast sotsiaalmeedias.

. . . . . .

. . . . . .

. . . . . .

Mida faktikontrollijatelt õppida

Pipsa Havula

Faktide kontrollimine algab alati sama põhiküsimusega: **kas tõesti?** Kui uudishimu on tekkinud, hakatakse väidet kontrollima.

Uurimused näitavad (1), et viis, kuidas faktikontrollijad digiplatvormidel uuele teabele lähenevad (seda nimetatakse lateraalseks ehk kõrvutavaks lugemiseks), on osutunud väga tõhusaks. Traditsiooniline lugemine ja tekstianalüüs ei pruugi digikeskkonnas tõhusad olla, sest kui lugejad hakkavad tundmatut võrguteavet analüüsima esmalt artikli allikat kontrollimata, ei pruugi nad aru saada, et kogu tekst põhineb kallutatud või täiesti eksitaval teabel. Lateraalselt lugedes kontrollib lugeja veebiteabe tausta eri saitidelt ja allikatest, enne kui hakkab sellesse süvenema. Varem tundmatu veebiteabega kokku puutudes avavad faktikontrollijad brauseris kohe mitu vahekaarti ja otsivad teavet organisatsiooni või selle taga oleva isiku kohta.

Kui keskmine lugeja võib kulutada märkimisväärse hulga aega lugemisele ja ebaõige teabe üle mõtlemisele, siis faktikontrollijad kasutavad nn strateegilist eiramist. Pärast kiiret kontrolli jäetakse kahtlasteks ja ebausaldusväärseteks osutunud veebiallikad kõrvale. Eeldus on, et teabe kvaliteet on kehv, kuni ei ole tõestatud vastupidist.

Kõige lihtsamalt selgitades: kui faktikontrollija leiab uue veebiajalehe (nt Daily Mail), avab ta kohe brauseris uue vahekaardi, sisestab otsingumootorisse ajalehe nime ja lisab sõna „usaldusväärsus" või „erapoolikus" (nt Daily Maili usaldusväärsus) ning uurib tulemusi, otsides teavet, mis aitab veebisaidi või uudise teksti usaldusväärsust hinnata. Samal ajal saab vaadata, milliseid artikleid see väljaanne on varem avaldanud, kes ajakirja eest vastutab ja selle tekste levitab.

Kõrvutav lugemine toimib ka sotsiaalmeediaplatvormide pildi- ja videovoogude sirvimisel. Kui uudishimu on tekkinud, hakkab faktikontrollija uurima eri allikaid, et selgitada välja, kes on väite avaldanud, võimalikud motiivid ja näiteks selle, kus sama pilti või videot on varem avaldatud. Piltide ja videote tõepärasuse kontrollimiseks on hulk tasuta veebitööriistu, mida kirjeldatakse üksikasjalikumalt artikli lõpus.

Faktikontrollijate töömeetodid on muutunud digitaalse infopädevuse oluliseks osaks. Õnneks saab neid oskusi õppida, õpetada ja arendada ning FaktaBaari faktikontrollijad on sellesse artiklisse kokku kogunud mõned enda ja oma kolleegide näpunäited allikakriitilisuse arendamiseks. Täiendame selles käsiraamatus sisalduvaid artikleid õppevideotega RaRa veebilehel: https://www.rara.ee/uuri/desinformatsioon/

Sissejuhatus faktikontrollimise protsessi ja metoodikasse

Faktikontroll on protsess, mille käigus kontrollitakse, kas avalikkusele esitatud väide vastab tõele või mitte. Faktikontroll aitab eristada valesid, moonutatud, eksitavaid või halvasti põhjendatud väiteid usaldusväärsest, tõele vastavast teabest.

Uurimiskeskuse Duke Reporters' Lab (2) andmetel on praegu umbes 105 riigis üle maailma 400 uurijate ja ajakirjanike meeskonda, kes tegelevad faktikontrolliga. Euroopas on üle 110 faktikontrollitalituse. Mõned neist tegutsevad sõltumatult, mõned traditsioonilise uudismeedia osana ja mõned näiteks mõttekodade koosseisus.

Faktikontrolli on vaja, kuna vale või eksitav teave võib kõigutada inimeste arusaamu ja mõjutada nende tegutsemist. Eurobaromeetri andmetel peab 83% eurooplastest võltsuudiseid ja desinformatsiooni ohuks demokraatiale. Maailm on näinud, kuidas desinfo võib mõjutada valimisi, kaotada usalduse institutsioonide vastu, õõnestada sõnavabadust või isegi vähendada valmisolekut end vaktsineerida. Väidete kontrollimine usaldusväärsetest allikatest pärineva usaldusväärse teabe abil on üks tõhus viis väärinformatsiooni vastu võitlemiseks.

Siiski on oluline meeles pidada, et väidete tõlgendamine ei ole alati ühene ja et ka fakte võib tõlgendada erinevalt. Seetõttu püütakse faktide kontrollimisel teabe allikas võimalikult selgelt ära näidata, et lugeja saaks allikate usaldusväärsuse üle ise otsustada ja asjast oma arvamuse kujundada.

Piltide ja videote autentsuse kontrollimine

Veebis ringi vaadates satute sageli piltidele ja videotele, mis tekitavad küsimusi. Kas seda on töödeldud? Kus ja millal see filmiti? Mis videol või pildil tegelikult toimub?

Pildi või video autentsust ei ole alati lihtne kontrollida ja mõnikord võib see isegi võimatu tunduda. Tehnoloogia areneb aga pidevalt ning koos piltide ja videote töötlemise lihtsamaks muutumisega muutub lihtsamaks ka nende tõelevastavuse kontrollimise tehnoloogia. Igaüks saab kasutada tasuta veebipõhiseid faktikontrollivahendeid, mida faktikontrollijad oma igapäevatöös kasutavad.

Oluline on meeles pidada, et alati ei ole tegemist olukorraga, kus videot või pilti on töödeldud, vaid materjal on täiesti autentne, kuid esitatud vales kontekstis.

Pildid

Pöördpildiotsing (ingl *reverse image search*). Eri teenusepakkujate pöördpildiotsingud on sageli parimad vahendid, mille abil foto kontrollimist alustada. Pöördpildiotsingus laaditakse üles või lingitakse vaadeldav pilt, et otsimootor saaks leida sarnaseid pilte. Seda võtet saab näiteks kasutada, et välja selgitada, kus ja millal konkreetne foto on tehtud, kus sama foto on varem avaldatud või isegi kindlaks teha pildil oleva isiku või hoone. Algallikat otsides tasub vaadata piltide resolutsiooni: tavaliselt juhatab kõrgeima resolutsiooniga pilt su algse avaldamiskoha juurde.

Kõige lihtsam viis pöördpildiotsinguks on kasutada Google Lensi. Paremklõpsa pildil – siis saad otsida pilti Google Lensi abil.

Google'i pöördpildiotsingut kasutades saad määrata ajavahemiku, mille kohta pilte otsid. Google lisab pildiotsingu järele alati märksõna ja otsingutulemuste muutmiseks peaksid seda muutma. Bing tunneb ära pildil oleva teksti ja sorteerib pildid suuruse järgi, TinEye võimaldab aga pildid kronoloogilisse järjekorda panna.

Pildi metaandmed. Pildid salvestavad mitmesuguseid metaandmeid. Metaandmed võivad sisaldada foto tegemise kuupäeva ja kellaaega. Kui pilt on originaal, sisaldab see tõenäoliselt ka sellist teavet nagu näiteks foto tegemiseks kasutatud kaamera või telefoni mudel. Mõnikord, kuigi harva, sisaldavad metaandmed ka pildi tegemise koha GPS-koordinaate.

Väikesed vihjed. Pildilt tasub otsida väikseid detaile ja vihjeid. Kas seal on näiteks näha sildid, lipud, autode numbrimärgid, ilmastikuolud, äratuntavad ehitised või maamärgid? Kas on võimalik teha järeldusi sellest, milliseid riideid pildil olevad inimesed kannavad?

Kui pildil on võõrkeelne silt piisavalt selgelt näha, saad sildi kujutise üles laadida Google Translate'i, mis teksti ära tõlgib. Veebisaidil Wolfram Alpha (wolframalpha.com) on võimalik vaadata ilmastikuolusid konkreetsel päeval konkreetses kohas. Kaarditeenused aitavad leida täpse koha, kus pilt tehti.

Videod

Paljud ülaltoodud meetodid toimivad ka videote korral: väikeste vihjete otsimine, pöördpildiotsing ja metaandmed aitavad sageli õigele teele jõuda.

Pöördpildiotsing. Pöördpildiotsingut on võimalik teha ka videoga, tehes sellest ekraanipildid ja laadides need üles pöördpildiotsingusse. Brauserisse paigaldatud pistikprogramm InVid (3) aitab teha mitut pöördpildiotsingut video eri osadest korraga. Tööriist võimaldab vaadata ka video metaandmeid, näiteks salvestamise kuupäeva.

Vaata ja kuula. Palju räägitakse süvavõltsitud videotest, mis näevad välja nagu päris. Süvavõltsitud videotes kasutatakse pildimanipulatsiooni, et panna inimene ütlema või tegema asju, mida ta tegelikult ei ole öelnud ega teinud.

Süvavõltsingutest sagedamini on videopettuste puhul tavaline, et tegelikku videot on näiteks eksitavalt lõigatud, et luua kõneleja räägitust moonutatud ettekujutus. Selline töötlus võib olla väga peen ja oskuslik, mistõttu on seda raske avastada.

Originaalvideot on võimalik leida pöördpildiotsingu või otsingumootori abil ning on ka veel teisi võimalusi. Videot hoolikalt vaadates, heli kuulates ja veidraid katkestusi (hüppeid) otsides on võimalik kindlaks teha, milliseid osi on manipuleeritud. YouTube'i või Vimeosse üles pandud video saab linkida veebisaidile watchframebyframe.com ja vaadata iga kaadrit aeglustatult. Nii on üllatavaid hüppeid lihtsam märgata.

Võõrkeelse video tõlkimine. Üks väärinformatsiooni levitamise viis on videote vale subtiitrimine ja võõrkeelse video asetamine täiesti valesse konteksti. Kui video on näiteks vene keeles ja vaataja seda keelt ei oska, on lihtne kasutada fiktiivseid subtiitreid või konteksti, et esitada tõele mittevastavaid väiteid.

Videot saab aga endale arusaadavasse keelde tõlkida. Vaja on vaid kahte eri seadet, näiteks nutitelefoni ja sülearvutit. Google Translate'i rakendus, mis suudab kõnet tuvastada ja tõlkida, on nutitelefoni laaditud. Teises seadmes esitatakse videot ja heli ning telefonis olev Google Translate kuulab kõnet ja tõlgib selle soovitud keelde. Tõlketeenused ei ole täiuslikud, kuid video konteksti või kõne ligikaudset tähendust on võimalik selle meetodi abil mõista.

Viited

(1) Wineburg, S., Breakstone, J., McGrew, S., Smith, M., & Ortega, T. (2022). Lateral Reading on the Open Internet: A District-Wide Field Study in High School Government Classes. Journal of Educational Psychology. https://psycnet.apa.org/fulltext/2022-53872-001.pdf

(2) Duke Reporters' Lab. https://reporterslab.org/fact-checkers-extend-their-global-reach-with-391-outlets-but-growth-has-slowed/

(3) InVid. https://www.invid-project.eu/tools-and-services/invid-verification-plugin/

Ülesanded

1. Mida tähendab kõrvutav lugemine?

2. Mida teed, kui kohtad tundmatut/uut infoallikat?

3. Nimeta veebilehti ja tööriistu pildi kontrollimiseks.

4. Mine lehele err.ee ning kontrolli esimese uudise pilti.

Kuidas hinnata teaduslikku väidet ja eksperdi pädevust?

Kari Kivinen

Oluline on meeles pidada, et veebis levib igasugune sisu. Õige ja kasuliku teabe kõrval on ka suur hulk ebaõiget teavet (valeinformatsiooni, st heauskselt või ekslikult levitatavat ebaõiget teavet) ja võltsitud teavet (desinformatsiooni, st tahtlikult levitatavat ebaõiget või ebatäpset teavet). Ebaõige või võltsitud teabe levitamine on sageli kahjulik nii üksikisikule kui ka kogukonnale. Seetõttu on kasulik kindlaks teha, kes on teabe taga, ning kontrollida teavet mitmest allikast, et mõista allika vaatenurka ja võimalikku erapoolikust.

Aeg-ajalt peame hindama sotsiaalmeedias avaldatud teadusuudiste usaldusväärsust: näiteks kas on olemas teaduslikud tõendid, et maskide kandmine on kasulik? Kas me saame kliimamuutuse peatada? Kas tuumaenergia on ohutu ja kas see on kestlik valik? Tänapäeva teadus on nii spetsialiseerunud, et ükski inimene ei suuda vallata kõiki valdkondi ja teemasid. Seetõttu sõltume ekspertidest ja peame hindama, kelle pädevusele võime toetuda – eriti kui ekspertide arvamused on mõnevõrra vastuolulised. Desinfo on sageli maskeeritud usaldusväärseks pseudoteaduslikuks väiteks. Tooteid võidakse turustada eksitavate või olematute viidetega mitmesugustele uurimustele, sotsiaalmeedias levitatakse kahtlase teadusliku kvaliteediga artikleid.

Kuidas eksperdi pädevust hinnata?

Kui valime advokaati, torumeest, hambaarsti või arhitekti, otsime tõendeid ja viiteid tema kogemuse, kutseoskuste ja kvalifikatsiooni kohta. Kuidas aga hinnata teadlase pädevust ja autoriteeti – kas ta on tuntud ja tunnustatud ekspert oma valdkonnas ja millised on tõendid tema pädevuse kohta?

Teadlase pädevuse kriteeriumid on samad, mis teiste ekspertide puhul. Oluline on välja selgitada (1):

- Millised on nende kogemused ja eelkõige nende teadusartiklid selles valdkonnas?
- Kas nad on oma valdkonnas tunnustatud? Kas nad on näiteks tunnustatud teadusasutuse töötajad või oma teadustegevuse eest auhindu saanud? Igas kutseliidus on oma „valvurid", juhatused ja sertifitseerijad, kes jälgivad oma liikmeid, et nad tegutseksid vastavalt kutseala standarditele ja tagaksid selleks vajaliku kvalifikatsiooni.
- Milline on nende kvalifikatsioon? Kas see on doktorikraad asjaomases valdkonnas või on neil peale ametliku kvalifikatsiooni ka muid valdkondlikke kogemusi?
- Kus nad töötavad? Kas see on tunnustatud teadusasutus?
- Kas on tõendeid võimaliku erapoolikuse või rahaliste huvide kohta?

Teadlaseks olemine nõuab aastatepikkust õppimist ja sageli ka doktorikraadi, kuid isegi doktorikraad katab vaid kitsast teadmiste valdkonda. Pädevuse võib omandada ka teadusliku erialakoolituse või praktilise töökogemuse kaudu.

„Ainult praktiseerivast teadustegevusest siiski ei piisa. Isik peab olema praktiseeriv teadlane asjaomases valdkonnas. Nobeli preemia saamine ühes valdkonnas ei tee kellestki eksperti teistes valdkondades. Ometi võivad inimesed kergekäeliselt kõik teadlased ühte patta panna kui eristamata autoriteedid. Radioloogiaspetsialist ei ole keegi, kellelt viiruste kohta nõu küsida. Ühe valdkonna teadlane olemine ei tee kellestki eksperti teistes valdkondades. Teoreetilise kosmoloogia spetsialist ei tea ökoloogiast rohkem kui mõni teine pädev kõrvalseisja.” (1).

Sotsiaalmeedias on välja ilmunud eksperdid, kes kommenteerivad Venemaa sissetungi Ukrainasse. Sageli on nende avaldustest olnud lihtne järeldada, kumba poolt nad esindavad. Konflikti ajal tuleb seetõttu uudistesse ja ekspertarvamustesse suhtuda tavapärasest ettevaatlikumalt ja kaalutletumalt. Oluline on välja selgitada, kes mida esindab, millistel tõenditel teave põhineb ja milline on avalduse tegija tegelik pädevus kõnealuses küsimuses.

Kuidas teaduslikku väidet hinnata?

Teaduslik informatsioon peab läbima mitu protsessi, et selle usaldusväärsus saaks kinnitatud. Avatus, kriitiline arutelu ja eelretsenseerimine viivad teadust edasi. Teadus ka parandab iseennast. Teadusandmete tõlgendusi muudetakse ja täpsustatakse sedamööda, kuidas uusi teadmisi lisandub. Teadus tugineb aastakümnete, kui mitte sajandite jooksul kogutud teadmistele.

Teaduslikud teadmised on meie praegune parim arusaam asjadest. See ei ole kellegi arvamus ega isiklik kogemus, vaid saadud süstemaatilise tegevuse tulemusel. Teadmised võivad muutuda, kui saadakse uusi uurimistulemusi ja tekivad uued arusaamad, seetõttu on uurimustel põhinev teadus rohkem väärt kui arvamused!

Teaduspõhise väite korral tasub uurida, kas väidet esitaval isikul või organisatsioonil on huvide konflikt. Kas kaalul on majanduslikud, usulised või poliitilised huvid? Kui jah, siis võib tegemist olla tasulise reklaamiga ja tulemustesse tuleks suhtuda kahtlevalt. Näiteks tubaka- ja fossiilkütusetööstus on kasutanud oma palgal olevaid eksperte, et levitada ettevõtetele kasulikku teavet.

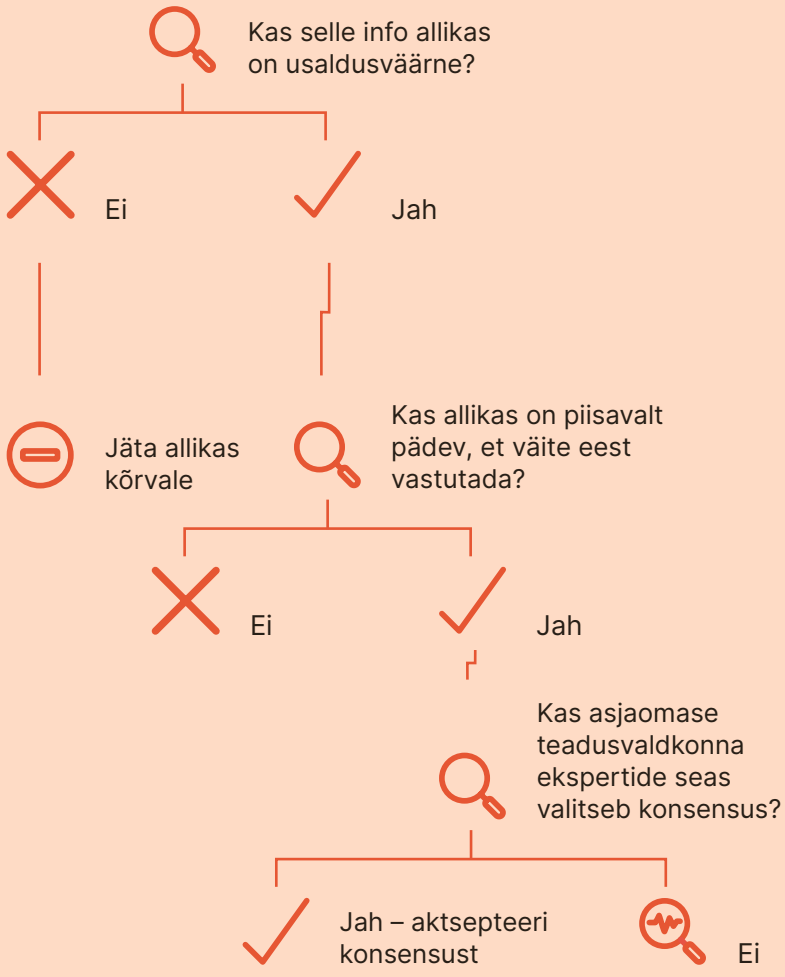
Kui huvide konflikti ei ole, tuleks esitada järgmised küsimused:

- Kas isik või organisatsioon on selles valdkonnas pädev?
- Milline on autori maine teadusringkondades?
- Kas ta on alati aus olnud?
- Kas autoril on asjakohane kvalifikatsioon või muud valdkondlikud kogemused?
- Kas ekspertide seas valitseb laialdane teaduslik konsensus? Kui ei, siis mida arvab enamik teadlasi?
- Kui kindel on teadusringkond oma väidetes?
- Kas ja millisel määral on ühesugused eksperdid seda järeldust kontrollinud?

Samuti tasub leida hetk, et kaaluda võimalikku kasu ja riske. Näiteks pidime koroonaajal tegema isiklikke valikuid, kas järgida ekspertide nõuandeid, näiteks kas vaktsineerida end COVID-19 vastu, kanda maski, arvestada karantiiniperioode ja pidada koduseid teste usaldusväärseteks.

Eri riikide faktikontrollijatel on huvitavaid veebilehti, kust saab teada, kuidas nad kontrollivad näiteks väidete õigsust ning piltide ja videote autentsust ja algupärasust. EDMO faktikontrollijate kogukond on koostanud ajakohastatud loetelu usaldusväärsetest Euroopa faktikontrolli organisatsioonidest. Eestis on Eesti Päevaleht koostanud „Valeinfo: paljastatud” materjalid, teemaga tegelevad ka Propastop ja Eesti Väitlusselts.

Otsustuspuu teadusinfo hindamiseks



Tõendid usaldusväärsuse kohta:

- Kas puudub huvide konflikt?
- Kas on vaba ideoloogilistest eelarvamustest?
- Kas on poliitiliselt neutraalne?
- Kas allikad on tunnustatud?

Tõendid pädevuse kohta:

- erialased tulemused
- maine kolleegide seas
- kvalifikatsioon või kogemused
- institutsiooniline kontekst

Küsi selgituste, tõendite iseloomu või kindlusastme kohta

Otsi infot ebakindluse puhul:

- Millised on erimeelsused või milles on eksperdid ühel arvamusel?
- Mida arvavad kõige kõrgemalt hinnatud eksperdid?
- Milliseid tulemusi peetakse usutavaks?
- Millised on eksimise riskid?

Joonis. Skemaatiline ülevaade meetodist, mida meie arvates tuleks kasutada internetis esitatud teaduslike väidete hindamisel (1)

Viited

(1) Osborne, J., Pimentel, D., Alberts, B., Allchin, D., Barzilai, S., Bergstrom, C., Coffey, J., Donovan, B., Kivinen, K., Kozyreva, A., & Wineburg, S. (2022). Science Education in an Age of Misinformation. Stanford University, Stanford, CA. https://sciedandmisinfo.stanford.edu/

Ülesanded

1. Milliseid kahtlasi, väärinfona tunduvaid väiteid oled viimasel ajal meedias märganud?

2. Palun uuri, milline haridus ja taust on Rainer Saksal ja Sergei Metlevil, et neid arvamusliidriteks nimetatakse.

3. Palun vaata veelkord otsustuspuud ning pane kirja sammud, mida juba tegid ja mida kavatsed edaspidi teha.

Teadlikkus algoritmidest – tehisintellekti väljakutsed

Harto Pönkä

Tänapäeval seostatakse algoritmide mõistet peamiselt programmeerimise ning veebiteenuste ja -rakenduste funktsioonidega. Algoritm on aga algselt matemaatiline mõiste. Üldiselt tähendab algoritm sisuliselt ikkagi ühte ja sama: see on rida samme, mille abil lahendatakse probleem või ülesanne.

Tavaliselt arvatakse, et algoritmid töötavad automaatselt, kuid algselt olid need manuaalsed, st neid teostasid inimesed, näiteks koolides õpetatav võrrandi lahendamine täisarvuga korrutades või jagades. Samamoodi on kokaraamatus olevad retseptid algoritmid, mis õpetavad, kuidas valmistada teatavatest koostisosadest maitsvaid roogi, järgides selleks teatavaid samme.

Algoritmi iseloomustab asjaolu, et see kasutab soovitud tulemuse saamiseks sisendit, näiteks lähteelemente või -andmeid. Soovitud tulemuse määrab algoritmi looja. Programmeerimises viidatakse sellele mõistetega „sisend" ja „väljund", mille vahel toimub programmi tegelik täitmine.

Arvutiprogrammi algoritmid

Kõige levinumad algoritmid, mida arvutid kasutavad, on näiteks failivormingud, mida kasutatakse piltide, helide ja videote salvestamiseks ja kokku pakkimiseks. Näiteks saab digitaalse foto JPEG-pakkimisalgoritmi abil kokku pakkida murdosani selle füüsilisest failisuurusest. Algoritme kasutatakse ka otseülekande võrgu kaudu vaatajatele edastamisel või otsijale internetiserveri kaudu konkreetse veebilehe edastamisel, kui ta on selle aadressi brauserisse sisestanud.

Mõnikord on väljundandmed ning algoritmide võtted ja tulemused väga keerulised; tavaliselt seetõttu, et algoritmi sisendandmed koosnevad suurest hulgast varem kogutud andmetest või kuna ühe ülesande täitmiseks kasutatakse suurt hulka eri muutujaid või andmepunkte.

Näiteks saab prognoosida konkreetse piirkonna ilma, kasutades selleks varem kogutud andmeid nagu temperatuur, sademed, tuul, õhurõhk ja vaatlustel põhinevad statistilised mudelid. Tänapäeva ilmaprognoosimudelid põhinevad aga prognoositava piirkonna virtuaalsel modelleerimisel, mis simuleerib tegelikke atmosfäärinähtusi. Sellist modelleerimist kasutavad algoritmid põhinevad tegeliku maailma peegelpildil.

Digikaksikud ja soovitussüsteemid

Kui algoritme kasutatakse inimese käitumise prognoosimiseks ja mõjutamiseks, nimetatakse tulemust vahel digikaksikuks. Nimetus viitab isiku ja tema tegevuse kohta kogutud andmete kogumile ning eri allikatest saadud andmete kombineerimisele. Näiteks on veebireklaamivõrgustike ja sotsiaalmeediasisu voogedastussüsteemide kasutatud soovitusalgoritmide eesmärk pakkuda igale kasutajale kõige sobivamat valikut olemasolevate andmete põhjal.

Soovitussüsteemid koondavad andmeid, mis on kogutud kasutajate ja kõigi soovituste kohta. Kõige tuntum soovitussüsteem on Google. Google'i otsing põhines algselt PageRanki algoritmil, mille mõte seisneb selles, et iga veebilehe väärtust mõõdetakse

selle järgi, kui paljud teised veebisaidid seda lingivad. Samal ajal mõjutavad PageRanki väärtust linkivate veebisaitide endi PageRanki väärtused, samuti teemade vastavus linkide sihtleheküljele.

PageRank on praegu vaid üks paljudest Google'i otsingus kasutusel olevatest algoritmidest. 2004. aastast on Google'i otsingutulemusi mõjutanud kasutajatelt kogutud andmed otsingutulemuste personaliseerimiseks, st eri kasutajatele erinevate veebilehtede soovitamiseks. 2010. aastaks teatas Google, et kasutab otsingutulemuste personaliseerimiseks rohkem kui 250 muutujat.

Praegu mõjutavad Google'i otsingutulemusi muuhulgas kasutaja vanus, sugu, perekond, amet, hobid, asukoht, veebiostud, reisimine, huvid ja veebiajalugu. Google'i soovitusalgoritmid ei piirdu ainult otsingutulemustega, vaid neid kasutatakse ennekõike Google'i reklaamisüsteemis, et valida kasutajatele sobivaid reklaame. Paljudele tuleb üllatusena, et soovitusalgoritmid valivad ka uudiseid, mida kasutajad näevad, näiteks Androidi uudiste vaates.

Tehisintellekti algoritmid

Kui algoritm kasutab masinõpet või mõnda muud tehisintellekti tehnikat, nimetatakse seda tehisintellekti algoritmiks. Masinõpe tähendab, et algoritm ei anna iga kord sama tulemust, vaid seda treenitakse pidevalt uusi andmeid kogudes, nii et see „õpib" pidevalt oma tulemusi parandama.

Kõige tuttavam näide õppiva soovitusalgoritmi kohta on ilmselt YouTube'i algoritm, mis soovitab kasutajatele, milliseid videoid järgmisena vaadata. YouTube'i soovitusi mõjutavad varem vaadatud videod ja muud Google'i kogutud andmed, samuti potentsiaalsete soovitatud videote andmed, näiteks teemad ja keskmine tegelik vaatamisaeg. Aga selle asemel, et soovitada ainult varem vaadatud videote teemadega seotud uusi videoid, pakub YouTube'i algoritm ka videoid teemadel ja kanalitel, mida kasutaja ei ole veel vaadanud.

YouTube'i tehisintellekti algoritmi jaoks on iga videoettepanek nagu kasutajale suunatud katsetus, millest algoritm püüab õppida uut teavet: kõnealusel juhul seda, millised videoteemad kasutajat huvitavad ja millised mitte. Sarnast andmekogumist kasutavad paljud sotsiaalmeediateenused, näiteks Facebook, Instagram, X ja Spotify.

Hoolimata jõupingutustest töötada välja algoritmid, mis kasutajate erinevaid huve arvesse võtavad, kipub kasutajate tegevus ikka veel viima algoritmideni, mis annavad ühekülgseid soovitusi kitsastel teemadel. Näiteks kui sa klõpsad korduvalt Facebooki ja Instagrami kindlateemalistel postitustel, näed üha rohkem sama tüüpi sisu. Seda nähtust nimetatakse algoritmi eelarvamuseks.

Tehisintellekti algoritmide puhul võivad eelarvamusi põhjustada ka masinõppes algselt kasutatud õppematerjalid, näiteks Google Translate'i algoritm, mida eri elukutsete korral kasutatakse nais- või meessoole viitavate isikuliste asesõnade tõlkimiseks.

Google'it süüdistati seetõttu isegi diskrimineerimises, kuigi just selline materjal oligi tehisintellekti õpetamiseks saadaval. Praegu pakub Google Translate selliste tõlgete korral kaks võimalust.

Facebooki algoritmid ja emotsioonid

Kõikidest sotsiaalmeediateenustest on Facebook teinud kõige suuremaid jõupingutusi, et oma uudisvoo algoritmis kasutajate emotsioone kasutada. Artiklite meeldivaks märkimine on olnud osa Facebooki funktsionaalsusest peaaegu selle loomisest alates. Emotikonide kasutamine sai tõelise hoo sisse 2016. aastal, kui Facebook tõi turule sellised reaktsioonid nagu „armastan", „hahaa", „ohhoo", „kurb" ja „vihane".

Enne nende emotikonide kasutuselevõtmist korraldas Facebook praktilise eksperimendi, et näha, kuidas erinevad postitused kasutajate tegevust ja emotsioone mõjutavad. Uuringus leiti, et positiivsed postitused tekitasid positiivseid emotsioone ja negatiivsed postitused negatiivseid emotsioone. Kasutades andmeid, mida emotikonidega väljendatud reaktsioonidest koguti, suutis Facebooki algoritm valida kasutajate uudisvoogudesse postitusi nende emotsionaalse seisundi alusel: näiteks kui kasutaja

märgib sageli ohhoo-reaktsioone, näeb ta rohkem postitusi, mis on saanud palju samasuguseid reaktsioone.

2017. aastast suurendati emotikonidega väljendatud reaktsioonide väärtust uudisvoo soovitusalgoritmis viie tavalise meeldimiseni. Ettevõtted ja teised algoritmiuurijad leidsid peagi, et väga emotsionaalseid postitusi tehes tõusid nad algoritmi tulemusel kasutajate uudisvoo tippu. Sellist tegevust, mis kasutab ära inimeste käitumist ja sotsiaalmeediateenuste algoritme, nimetatakse sotsiaalmeedia optimeerimiseks.

Eriti tõhusaks emotsiooniks Facebookis osutus nördimuse ja viha tekitamine. Enam kui kahe miljardi kasutaja juures mängivad algoritmide muutused suurt rolli: ühelt poolt kontrollivad nad seda, milliseid postitusi kasutajad näevad, ja teiselt poolt seda, milliseid postitusi mõjuisikud teevad. Nii et kui algoritm näis premeerivat viha õhutamist, hakkasid paljud sisuloojad selle põhjal tegutsema.

Vihasisu suur hulk on üks põhjusi, miks Facebooki on aastaid laialdaselt kritiseeritud. Facebook otsustas peagi alandada vihkamise emotikoni väärtust oma algoritmis: esmalt nelja meeldimiseni 2018. aastal, pooleteise meeldimiseni 2020. aastal ja lõpuks nullini 2021. aastal pärast seda, kui tuhanded dokumendid, mille lekitas Facebooki endine töötaja Frances Haugen, ülaltoodu paljastasid.

Kas algoritmidel on liiga palju võimu?

Facebooki algoritmide kohta ilmnenud andmed on hoogustanud arutelu, kas algoritmidel on veebiteenuste kasutajate üle liiga palju võimu. On tõsiasi, et algoritmid mõjutavad kasutajate käitumist. Kõige sagedamini avaldub see mõju kasutajatele soovitatud sisus.

Samal ajal on õigustatult kahtluse alla seatud, kas isegi algoritmide autoritel on alati kontroll selle üle, kuidas algoritmid töötavad. Eriti tehisintellekti algoritmid pakuvad mõnikord tulemusi, mida on raske ennustada.

Facebooki algoritmid on väga keerulised: ettevõte on kiidelnud, et kasutab kuni 10 000 andmepunkti, et valida, mida igale kasutajale näidata. Kui seda, mida kasutajad näevad, mõjutavad nii paljud tegurid, ei ole tervikut lihtne hallata.

On märkimisväärne, et kuigi Facebooki uudisvoo algoritm andis ebaproportsionaalselt suure nähtavuse näiteks desinformatsiooni, vaenu õhutamist ja klõpsusööta sisaldavatele postitustele, püüdsid ettevõtte enda moderaatorid sama tüüpi sisu välja juurida. Facebookil ei olnud aga piisavalt moderaatoreid, et eemaldada kõik kahjulikud postitused, mille algoritm uudisvoo tippu tõstis.

Kas algoritmide põhimõtted tuleks avalikustada?

Sageli nõutakse, et sellised võrguhiiud nagu Google, Facebook ja X peaksid oma algoritmide aluseks olevad põhimõtted avalikustama. Need nõudmised on peamiselt seotud algoritmide väidetava kahjulikkusega, näiteks nende püüdega maksimeerida aega, mida kasutajad sotsiaalmeedias veedavad, ning algoritmide probleemidega valeteabe leviku takistamisel ja vastandumise tekitamisel.

Veebi- ja sotsiaalmeediateenuste äri põhineb tavaliselt reklaamide rahaks muutmisel, st soovil, et kasutajad klõpsaksid neile suunatud reklaamidel. Ja sellist tegevust muidugi soodustab vajadus tagada, et nad jääksid seda sisu vaatama võimalikult kauaks. Seega on selge, et algoritmid on häälestatud tagama just seda, isegi kui teenusepakkujad seda ise ei tunnista. Teisalt näitavad paljud uuringud, et pikalt veebi ja sotsiaalmeedia kasutamine ei toeta kasutajate heaolu. Teenuseid pakkuvate ettevõtete ja kasutajate huvid ei lange algoritmide toimimisel kokku.

Internetihiiud ei ole soovinud avalikustada teavet algoritmide kohta, viidates ärisaladuse hoidmisele ning asjaolule, et algoritmide avalikustamine tooks kaasa nende kasvava väärkasutuse ja manipuleerimise sisu avaldajate ja teiste veebis tegutsevate mõjuisikute poolt. See väide on õigustatud, sest algoritmide arendamiseks ja ärakasutamiseks käib

pidev võidujooks. Teisalt võib väita, et veebihiidude ülesanne on töötada välja algoritmid, mis on piisavalt head, et tuvastada ja vältida manipuleerimiskatseid.

Algoritmide avatuse üle peetavates aruteludes unustatakse sageli, et mõned nende tööpõhimõtted on juba avalikustatud. Näiteks Google kirjeldab põhjalikult ja samas üldiselt tegureid, mis mõjutavad tema tulemusi. Google on avaldanud ka ligi 200-leheküljelise juhendi, mis on kättesaadav kõigile ja mida saavad kasutada ka tema enda otsingutulemuste hindajad. Samuti on Google loonud mitu vahendit veebisaitide arendajatele, et testida ja parandada nende saitide jõudlust ja samal ajal nende järjestust Google'i otsingutulemustes. Võib öelda, et Google on hea näide algoritmide läbipaistvusest. Teisalt ei saa me kuidagi teada, mida Google meile ei ütle.

Lihtne on olla skeptiline selle suhtes, kui paljud veebiteenuste kasutajad viitsivad lugeda sadu lehekülgi dokumente, milles kirjeldatakse algoritmide üksikasjalikku toimimist. Põhimõtteliselt on see siiski oluline teema. Kui algoritmide tööpõhimõtted avalikustataks, siis suureneks teadlikkus, seni varjatud mehhanismid saaksid nähtavaks ja teadlased saaksid neid palju põhjalikumalt uurida. Kasutajate privaatsuse seisukohast oleks kõige tähtsam teada, kuidas nende isikuandmeid algoritmides kasutatakse. Seepärast on väljatöötamisel uued ELi õigusaktide paketid, millega nõutakse veebiandmete pakkujatelt suuremat läbipaistvust algoritmide toimimise osas.

Viited

Google (2022). Miten tulokset luodaan automaattisesti.
https://www.google.com/intl/fi/search/howsearchworks/how-search-works/ranking-results/

Google (28.7.2022). Search Quality Evaluator Guidelines.
https://static.googleusercontent.com/media/guidelines.raterhub.com/fi//searchqualityevaluatorguidelines.pdf

Pönkä, H. (31.10.2021). Infografiikka: Facebookin viha-reaktio ja algoritmin muutokset.
https://harto.wordpress.com/2021/10/31/infografiikka-facebookin-viha-reaktio-ja-algoritmin-muutokset/

The Washington Post (26.10.2021). A whistleblower's power: Key takeaways from the Facebook Papers.
https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/

Wikipedia (2022a). Luettelo algoritmeista. https://fi.wikipedia.org/wiki/Luettelo_algoritmeista

Wikipedia (2022b). Tekoäly. https://fi.wikipedia.org/wiki/Teko%C3%A4ly

Wired (22.2.2010). Exclusive: How Google's Algorithm Rules the Web. https://web.archive.org/web/20110612022158/
http://www.wired.com/magazine/2010/02/ff_google_algorithm/2

Yle (19.12.2016). Näin sinua ohjataan Facebookissa ja internetissä.
https://yle.fi/aihe/artikkeli/2016/12/19/nain-sinua-ohjataan-facebookissa-ja-internetissa

Yle (12.2.2020). Hölkkääjä päätyy ultrajuoksuvideoihin ja kasvisruuan ystävä vegaanisisältöihin – Youtuben algoritmin tehtävänä on katsojan koukuttaminen. https://yle.fi/aihe/artikkeli/2020/02/12/algoritmin-tehtavana-ei-ole-totuuden-etsiminen-vaan-ihmisten-pitaminen-sivuilla

Ülesanded

1. Palun too mõned näited algoritmide kasutamisest.

2. Millised on digikaksiku plussid ja miinused?

3. Mõtle välja loominguline viis, kuidas sotsiaalmeedia algoritmid segadusse ajada, et saaksid oma uudisvoogu erinevaid uudiseid, mitte ainult ühekülgseid, mida algoritm soovitab.

Digitaalne jalajälg ja privaatsus veebikeskkonnas

Harto Pönkä

Privaatsus on digiajastul üks olulisemaid põhiõigusi. See õigus põhineb ühelt poolt riiklikel seadustel ja Euroopa Liidu määrustel nagu ELi isikuandmete kaitse üldmäärus, ning teiselt poolt rahvusvahelistel lepingutel ja ÜRO inimõiguste deklaratsioonil.

Privaatsus tähendab eelkõige eraelu, kodu ja suhtluse kaitset, kuid digikeskkonnas on asjakohasem rääkida konkreetse isikuga seotud teabest, st isikuandmetest. Need on andmed, mis on salvestatud meie kasutatavatesse digiseadmetesse ja -teenustesse, näiteks otsingumootoritesse ja sotsiaalmeediaplatvormidele. Selliseid andmeid nimetatakse digitaalseks jalajäljeks.

Et olla digikeskkonnas täielikult informeeritud osaline ja võimeline oma privaatsust selles haldama, on vaja teada, kuidas seadmed ja teenused kasutajate kohta teavet koguvad. Samuti on oluline olla teadlik teiste kasutajate privaatsusest, et mitte tahtmatult rikkuda nende privaatsust digikeskkonnas.

Digitaalse jalajälje võib jagada aktiivseks ja passiivseks. Aktiivne digitaalne jalajälg on teave, mille kasutaja on teadlikult lisanud või muul viisil veebis tekitanud. Passiivne digitaalne jalajälg on andmed, mida teenused koguvad kasutaja teadmata.

Aktiivset ja passiivset digitaalset jalajälge on keeruline eristada, sest teadlikkus andmete kogumisest sõltub kasutaja teadmistest. Sellegipoolest on kasulik teada, et sageli koguvad veebi- ja sotsiaalmeediahiiud andmeid kasutajate teadmata või viisil, mille teadvustamiseks on vaja digitaalse infopädevusega seotud eriteadmisi. Seetõttu on käesoleva peatüki

eesmärk anda lihtne ülevaade kõige tavalisematest andmete kogumise meetoditest ja tehnikatest.

Kellega on turvaline oma andmeid jagada?

Veebiteenused ja -rakendused nõuavad tavaliselt kasutajatunnuse loomist, st registreerimist. Enne uue konto loomist ja isikuandmete esitamist tasub kontrollida, kas teenust või rakendust haldav ettevõte tundub usaldusväärne ja kas sinu antud teavet hoitakse turvaliselt. Seda saab hinnata, otsides lisateavet ja teiste kasutajate arvustusi.

On hulk eksitavate nimedega rakendusi ja mänge, mis on loodud populaarsete rakenduste ja mängude põhjal. Need võltsrakendused on loodud ainult selleks, et kasutajatelt isikuandmeid koguda. Seetõttu tasub kontrollida, kas rakenduse autor on autentne,

ja lugeda teiste kasutajate kogemusi. Samuti on soovitatav mitte laadida rakendusi alla mujalt kui ametlikest poodidest. Halvimal juhul võivad alla laaditud rakendused sisaldada pahavara ja viiruseid, mis võivad andmeid varastada.

Kasutajanime registreerimisel on mõistlik mitte anda muud teavet kui see, mis on kohustuslik. Samuti võiks kaaluda, kas tasub veebiteenustele oma tegelikku sünnikuupäeva või nime anda. Kui see teave ei ole kasutustingimustes sõnaselgelt nõutud, ei ole fiktiivse teabe esitamine vale. Registreerimisvormid võivad olla teadlikult kujundatud selliselt, et kasutaja peaks andma enda kohta võimalikult palju teavet, isegi kui see ei ole teenuse kasutamiseks vajalik.

Kõiki unikaalseid andmeid nagu nimi, telefoninumber, e-posti ja kodune aadress võidakse kasutada teabe otsimiseks teistest allikatest. Hea soovitus on kasutada registreerimiseks teisest e-posti aadressi.

Paljude veebiteenuste korral, näiteks Google, Facebook ja Apple, saate registreeruda olemasoleva kasutajakonto abil. Need on samuti ainulaadsed teabekillud, mis tavaliselt võimaldavad koondada mujalt pärinevat teavet. Kui teenusepakkuja ei tundu usaldusväärne, on parem karta kui kahetseda.

Veebiteenuste ja -rakenduste kasutamine tekitab sageli personaalset ja konkreetse valdkonnaga seotud sisu. Iga postitus, meeldivaks märkimine ja kommentaar kogub meie kohta andmeid. Lisaks võimaldavad eelkõige sotsiaalmeediateenused suhelda teiste kasutajatega. Selle tulemusena satuvad kasutajakontod sageli petturite ja teiste küberkurjategijate sihtmärgiks. Sisselogimisel on alati hea mõte kasutada kaheastmelist autentimist, sest see pakub head kaitset häkkimiskatsete vastu.

Kuidas toimivad küpsised?

Veebiteenused ja -rakendused võivad salvestada kasutajate seadmetes küpsiseid ehk faile, mis sisaldavad kasutajate jälgimist võimaldavat teavet. Küpsiste kasutamise ja säilitamise aeg peaks alati olema teenuse juures märgitud. Kui tegemist on küpsistega, mis ei ole teenuse toimimiseks vajalikud, tuleb enne küpsiste kasutamist saada kasutaja nõusolek.

Olulised küpsised on näiteks need, mida kasutatakse sisselogimiseks ja kasutaja tehtud valikute salvestamiseks. Mitteoluliste küpsiste hulka kuuluvad reklaami, tegevuse jälgimise ja sotsiaalmeediaplatvormidega seotud küpsised. Sellised küpsised on tavaliselt seotud veebiteenuste poolt andmete kogumisega, et saada teavet kasutajate tegevuse ja huvide kohta, st profileerimiseks.

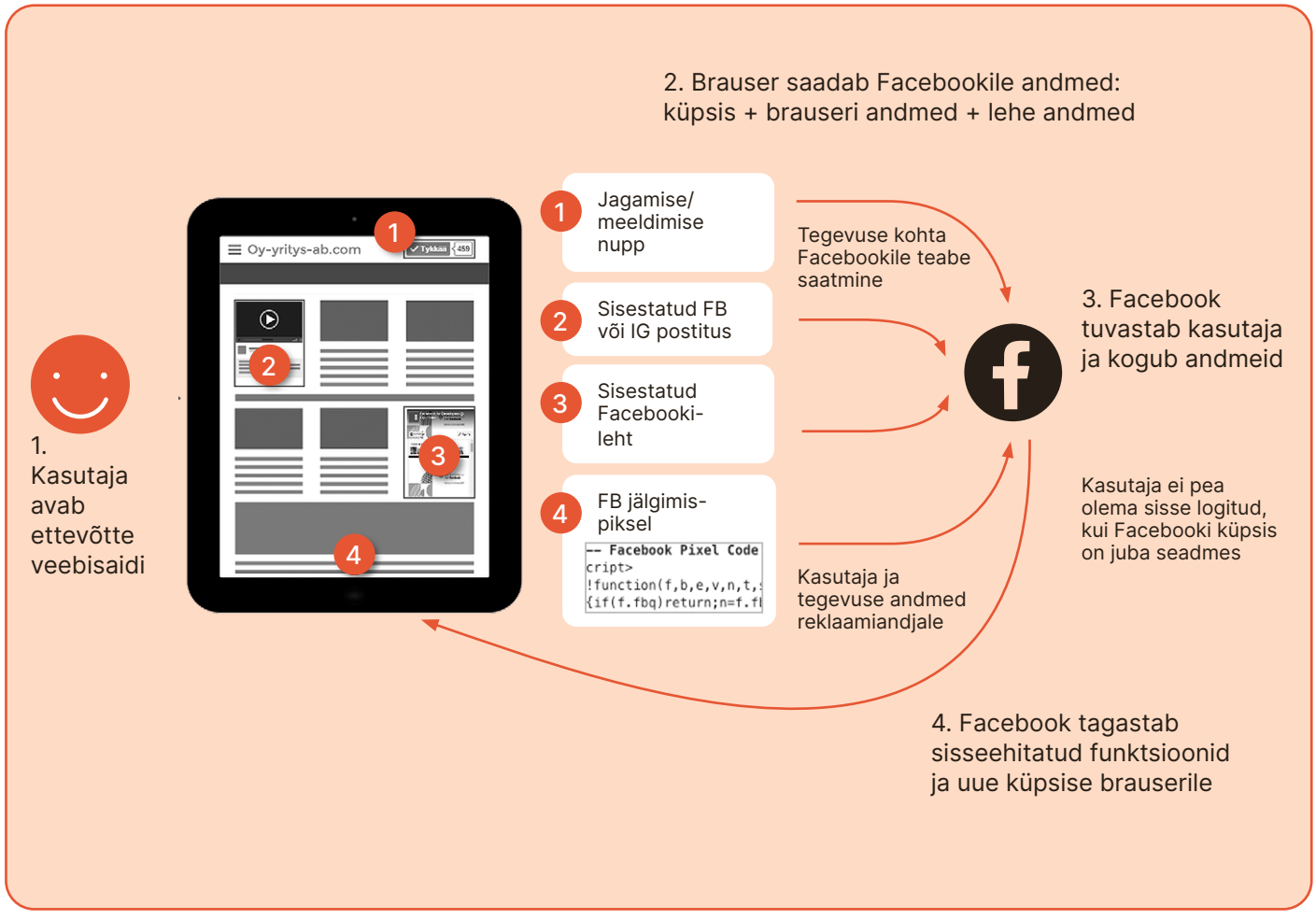
Näiteks kui kasutaja logib Facebooki sisse, salvestab küpsis teabe tema kasutajanime kohta. Facebookis on küpsis vajalik selleks, et kasutaja ei peaks oma kasutajanime ja parooli pidevalt uuesti sisestama. Sageli jäetakse aga tähelepanuta, et küpsis jääb seadmesse ka pärast Facebookist välja logimist, kui kasutaja seda otseselt ei kustuta.

Paljud sotsiaalmeedia- ja võrguteenused võivad integreerida funktsioone teistesse veebisaitidesse. Näiteks võib Facebook lisada ettevõtte veebisaidile meeldimisnupu või Facebooki jälgimispikslid, mis võimaldavad suunata veebisaidi kasutajatele Facebooki reklaami. Kui kasutaja sellist veebisaiti külastab, saadetakse seadmesse varem salvestatud küpsis automaatselt Facebookile, kui sisestatud funktsioon Facebooki serverist laaditakse. Kasutaja ei pea olema samal ajal Facebooki sisse logitud, kui küpsis on enne seadmesse salvestatud. Facebook saab küpsise sisu lugeda ja kasutaja selle sisu põhjal tuvastada. Samal ajal teab Facebook, millisel veebisaidil kasutaja on.

Facebook on võimeline kasutajate tegevust miljonite veebisaitide küpsiste kaudu pidevalt jälgima. See annab Facebookile andmeid selle kohta, mis kasutajaid huvitab, milliseid tooteid nad on hiljuti veebipoodides vaadanud jne. Neid andmeid kasutatakse reklaami suunamiseks Facebooki ja Instagrami reklaamplatvormil.

Google ja paljud teised veebiettevõtted kasutavad samuti küpsiseid kasutajate profileerimiseks. Küpsiste tavaline kasutusviis on nn pöördturundus (ingl *remarketing*), kus kasutajale näidatakse reklaami sama toote kohta, mida ta on varem veebipoes vaadanud.

Eri veebisaitide külastamisel peame praegusel ajal pidevalt vastama küpsiste kasutamise loa taotlustele.



Joonis. Kuidas küpsised toimivad. Facebooki näide

Tasub meeles pidada, et küsitakse ainult mitte-vajalike küpsiste kohta, mis tavaliselt ei ole kasutajale kasulikud, kuid mida võib põhjendatult pidada kahjulikuks ja privaatsust vähendavaks. Halvemal juhul võib üks veebileht saata küpsiseid ja muid jälgimisfunktsioone kasutades külastusandmeid kümnetele andmekogumisettevõtetele. ELis peavad võrguteenused pakkuma kasutajatele võimalust loobuda mitteolulistest küpsistest juba sisenemisel.

Küpsised ei ole ainus viis, kuidas veebiteenused võivad kasutaja seadmesse jälgitavaid andmeid salvestada. Teine levinud tehnoloogia on lokaalne salvestamine brauseris, jällegi on teenuse kasutamiseks vaja kasutaja nõusolekut. Peale selle töötab vähemalt Google välja tehnoloogiat küpsiste asendamiseks.

Kas asukohta tasub jagada?

Veebiteenused ja -rakendused võivad küsida kasutajatelt luba nende asukoha jälgimiseks. Näiteks võib uudisteportaal tuua põhjenduseks kasutajale asukohapõhise ilmaprognoosi näitamise, kuigi tegelikult kasutatakse asukohta ka sisu ja reklaami personaliseerimiseks.

Google'i otsingu ja reklaamivõrgu reklaamides kasutatakse asukoha jälgimist, et sellest järeldada, mis kasutajat huvitab. Google selgitab asukoha kasutamist järgmiselt: „Kui olete lubanud asukohta jälgida ja külastate sageli suusakeskusi, võite hiljem näha suusareklaami YouTube'i videos". Asukohaandmete kasutamist reklaamide suunamiseks saab aga hõlpsasti vältida, kui Google'i rakendustel ei lubata sinu seadme asukohta jälgida.

Seadme GPS-asukoht ei ole ainus viis kasutajate jälgimiseks. Asukoha robustsemaks või ebatäpsemaks määramiseks saab kasutada avalike WiFi-võrkude andmeid või kasutaja võrguühenduse IP-aadressi. Isegi sellist asukoha jälgimist saab vältida, kui kasutada internetti sisenemisel VPNi.

Peale veebiteenuste nõuavad juurdepääsu asukohainfole ka paljud mobiilirakendused. Tasub hinnata, kas rakenduses on funktsioone, mille puhul asukoha määramine on tõesti kasulik, ja otsustada, kas lubada sellel sinu asukohta jälgida. Samuti peaksid kontrollima oma telefoni seadeid, et näha, millistele rakendustele oled andnud asukoha jälgimise loa.

Seadme ja brauseri tunnused

Kui veebiteenuseid ja -rakendusi kasutatakse eri seadmetes ja veebibrauserites, võib neile määrata erinevaid unikaalseid tunnuseid. Näiteks Google ja Apple on oma reklaamisüsteemidele välja töötanud reklaamitunnused, mida kasutatakse kasutajate tuvastamiseks ja reklaami suunamiseks mobiilirakendustes. Need tunnused on olulised, kuna neid saab kasutada konkreetse seadme, näiteks mobiiltelefoni või tahvelarvuti sidumiseks konkreetse isikuga samamoodi nagu e-posti aadressi, telefoninumbrit või postiaadressi.

Kui identiteet on ühe rakenduse kaudu tuvastatud, saab seda seejärel tuvastada teistes samas seadmes kasutatavates rakendustes. On olemas arvukalt andmeettevõtteid, mis koondavad ja müüvad identiteedi- ja kasutajaandmeid kasutajate tuvastamiseks.

Veebibrauseritel ei ole sama unikaalset reklaamitunnuste süsteemi nagu mobiilseadmetel. Varem ei olnud see vajalik, sest küpsiste kasutamine oli väga vähe reguleeritud ja paljudel juhtudel oli kasutaja tuvastamine lihtne.

Kuna kasutajad on hakanud küpsiste kasutamist üha rohkem piirama, on andmekogumisettevõtted välja töötanud erinevaid brauseritunnuseid. Need märgised põhinevad erinevustel, mis esinevad brauseri konfiguratsioonides, näiteks seadetes, paigaldatud kirjatüüpides ja brauseri pistikprogrammides. Neid nimetatakse brauseri sõrmejälgedeks. See kirjeldab hästi nende eesmärki, st kasutaja tuvastamist tema kasutatava brauseri põhjal. Näiteks on teada, et rakendus TikTok on kasutanud oma veebiteenuses brauserispetsiifilisi pildi- ja helimärgiseid, mille abil saab kasutaja tuvastada isegi siis, kui ta ei ole teenusesse sisse logitud.

Ära jaga oma kontaktandmeid reklaamijatega

Kui kasutad Instagrami, Snapchatti, TikTokki või muid rakendusi, võidakse sinult küsida luba su kontaktandmete kasutamiseks. Tavaliselt põhjendatakse seda võimalusega leida oma sõpru, kes rakendust kasutavad, ja nendega ühendust võtta. Siiski ei ole soovitatav seda luba anda, kuna see kehtib kõigi sinu kontaktandmete kohta ja neid võidakse kasutada ka muudel eesmärkidel. Seega tasub veidi vaeva näha ja sõbrad, kellega soovid ühendust võtta, ise rakenduse kaudu üles otsida.

Kontaktandmed on samad andmed, mida veebi- ja sotsiaalmeediateenused kasutavad reklaami ja sisu suunamiseks, nagu ka muud andmed, mida nad sinu kohta koguvad. Need on võrguandmed, mis annavad sulle teada, kes on kellega ühendatud. Isegi kui me ei jaga oma kontaktandmeid sotsiaalmeediateenustega, võivad nad teiste jagatud kontaktandmete põhjal meie sõprade võrgustiku kohta teavet saada. Näiteks Facebook ja Instagram saavad seda infot kasutada uute sõprade ja jälgijate soovitamiseks.

Vahel kasutatakse kontaktandmeid ootamatutes olukordades. Näiteks ütleb Google, et kasutab kontaktandmeid algoritmis, mis soovitab uudiseid. Tõenäoliselt eeldab Google, et meid huvitavad samad teemad mis meie sõpru, kes loevad meiega sarnaseid uudiseid.

ELi isikuandmete kaitse üldmäärus annab kasutajatele palju õigusi, kui nad kasutavad teenuseid ELis.

Kui isikuandmete töötlemine põhineb kasutaja nõusolekul või kasutustingimustega nõustumisel, st lepingul, on kasutajatel vähemalt järgmised õigused, mida nad võivad kasutada:

- õigus saada teavet isikuandmete töötlemise kohta;
- õigus oma isikuandmetega tutvuda;
- õigus ebaõigeid andmeid parandada;
- õigus isikuandmed kustutada / õigus olla unustatud.

Jälgimine nn tumedas sotsiaalmeedias

Sotsiaalmeediateenustel on lihtne kasutajate suhtlust jälgida, kui see toimub nende enda teenustes. On selge, et näiteks Instagram jälgib, milliste kasutajate postitustele me reageerime, ja kasutab kogutud andmeid oma uudisvoo algoritmis.

Kasutajate tegevuse jälgimine sotsiaalmeediavälistes rakendustes on neile seevastu keerulisem. Üha enam jagatakse linke sotsiaalmeediapostitustele ja uudistele näiteks nn tumedas sotsiaalmeedias, mis viitab peamiselt sõnumirakendustele nagu WhatsApp, Snapchat ja Yodel.

Tavaliselt ei ole veebiteenuse pakkujal võimalik teada saada, kes on linki väljaspool teenust jaganud ja kellele. Paljud veebi- ja sotsiaalmeediateenused on aga välja töötanud meetodid linkidele tunnuste lisamiseks, mis võimaldavad neil teada saada, kes algselt linki jagas. Need märgised võivad olla näiteks #-koodi kujul, mis järgneb lingi tegelikule aadressile või nn lühendatud linkidele. Mitmed linkide koondamise teenused võimaldavad linkide jagamist jälgida.

Kui jagatud link avatakse, teavad veebiteenused lingi märgise järgi, kes seda linki jagas. Lisaks saavad veebiteenused sageli tuvastada lingi avanud kasutajad, näiteks küpsiste või muude eespool kirjeldatud vahendite abil. Selle tulemusena saavad nad ka teavet linkide jagamise kohta nn tumedas sotsiaalmeedias ja lisainfot kasutajate võrgustike kohta.

Kuidas andmeid kustutada?

Lihtsaim viis võrguteenuste ja -rakenduste kaudu kogunenud andmed kustutada on lihtsalt kustutada oma avaldatud sisu, teenuses salvestatud asukoha- või sirvimisajalugu, edastatud kontaktandmed või terve oma kasutajakonto. Tavaliselt sisaldavad kasutustingimused tingimust, et kui kasutaja oma andmed kustutab, ei tohi teenusepakkuja neid hiljem säilitada.

Paljud veebiteenused ja -rakendused võimaldavad sul kontrollida, millist teavet sinu tegevuse kohta salvestatakse ja kuidas seda kasutatakse. Need valikud leiad kasutajakonto seadetest. Näiteks Google'i kasutajakonto seaded võimaldavad loobuda reklaamide personaliseerimisest, et sinu kontole salvestatud andmeid ei kasutataks reklaamide suunamiseks.

Ülesanded

1. Palun lõpeta lause „Privaatsus kaitseb .....”
2. Kuidas inimesed internetis privaatset teavet jagavad? Vali õige variant.

   pildi postitamisega internetti

   postitades teate puhkuseleminekust

   luues sotsiaalmeediakonto

   kirjutades e-kirju

   olles Facebooki grupi/gruppide liige
3. Palun kirjelda, kuidas oma isikuandmeid kaitsta, kui mõne veebisaidi kasutajaks registreerud või registreerimisvorme täidad.

. . . . . .

. . . . . .

. . . . . .

4. Nimeta neli viisi, kuidas jätad endast digitaalse jalajälje.

. . . . . .

. . . . . .

. . . . . .

ŠVEITSI–EESTI
koostööprogramm

Autorid: Triin Nigul, Stella Saarts, Kari Kivinen, Carita Kiili, Minna Aslama Horowitz, Joonas Pörsti, Pipsa Havula ja Harto Pönkä

Sisaldab tõlkeid väljaandest „Digital information literacy guide. A digital information literacy guide for citizens in the digital age", Faktabaari EDU, 2022

Sisutoimetajad: Kristiina Kaju, Kateryna Botnar

Inglise keelest tõlkinud Luisa Tõlkebüroo

Keeletoimetanud Luisa Tõlkebüroo, Gerli Randjärv

Kujundajad: Viktor Gurov, Margit Plink

Kirjastaja: Eesti Rahvusraamatukogu

Trükikoda: Tallinna Raamatutrükikoda

Väljaanne on valminud projekti MeediaRadar raames, rahastus Šveitsi-Eesti koostööprogrammi toetusmeetmest „Sotsiaalse kaasatuse toetamine"

Võrguväljaanne: ISBN 978-9949-413-85-0 (pdf)

Trükis: ISBN 978-9949-413-83-6

RaRa EESTI RAHVUS-RAAMATUKOGU