Sensuurin uudet muodot

Päivikki Karhula

Elektronisten aineistojen ja verkkoympäristön myötä kysymykset sensuurista ovat alkaneet tulla monimutkaisemmiksi. Verkkosensuurin lisäksi voidaan puhua tietovalvonnasta ja laajemmin käyttäjien kontrollista verkossa. Sensuurin ja tietovalvonnan yhdistävillä menetelmillä voidaan seurata käyttäjiä ja heidän toimiaan verkossa, kontrolloida heidän pääsyään verkon sisältöihin ja puuttua heidän toimiinsa muilla tavoilla. Tässä kirjoituksessa kuvataan verkkosensuurin ja tietovalvonnan kehityskulkuja ja niiden seurauksia kirjastoille ja käyttäjille.

Sensuuri ei ole uusi ilmiöitä, vaan sitä on ollut olemassa siitä alkaen, kun on ollut painettuja julkaisuja. Sensuuri on perinteisesti kirjastoissa ymmärretty puuttumisena painettuihin julkaisuihin. Perustaltaan jo hankintapolitiikka voi olla sensuuria, jos on niin, että käytetään aatteellisia tai poliittisia määreitä siihen, millaisia aineistoja kirjastoon ei hankita. Sensuuri puuttuu ideologioihin, tiettyihin teemoihin tai tulkintojen näkökulmiin.

Tietovalvonnan kautta toimiva sensuuri toimii samankaltaisin periaattein, huomio kiinnitetään tietyntyyppisiin aineistoihin ja niiden käyttöön, mutta sen lisäksi huomiota kiinnitetään käyttäjiin. Teknologian kehityksen myötä sensuurin ja valvonnan menetelmistä tulee kuitenkin systemaattisempia. Haluttua seurantaa ja rajoituksia voidaan kohdistaa laajempiin ihmisryhmiin tai saada nopeasti jäljitettyä sisältöjen käyttötilanteita. Nykyisellään langattoman ja mobiiliteknologioiden ympäristössä tietovalvonnasta on tullut yhä tarkempaa, laajempaa ja ympärivuorokautista.

Verkkosensuuri ja tietovalvonta

Verkkosensuurilla voidaan vaikuttaa monin erilaisin tavoin julkaisujen tai sisältöihin pääsyyn. Kirjastojen osalta eniten on puhuttu suodatusohjelmista eli filtteroinnista, mutta sisältöihin pääsyä voidaan säädellä monilla muillakin menetelmillä, joiden lopputulokset ovat sensuurin luonteisia. Verkkoyhteyksiin, sisältöjen jakeluun tai sisältöihin pääsyyn voidaan puuttua tai aineistojen tuottajat tai käyttäjät voidaan jäljittää.

Yleiskäsitteenä voitaisiin puhua käyttäjien kontrollista, joka pitää sisällään verkkosensuurin ja tietovalvonnan. Verkkosensuuri on kontrollin suora muoto, jolla voidaan estää tai rajoittaa käyttäjän pääsyä haluttuihin sisältöihin. Sen lisäksi verkossa käytetään tietovalvontaa, jonka avulla voidaan seurata käyttäjän toimia ja hänen käyttämiään ja tuottamiaan sisältöjä.

Tietovalvonta on tietoon pääsyyn nähden välillistä sensuuria – käyttäjään voidaan haluttuja kohdistaa toimia sen perusteella, millaisista sisällöistä hän on kiinnostunut ja mitä tietoa hänen toimistaan verkossa on kerätty. Verkossa sensuuri voi myös toimia hyvin nopeasti ja tarkasti. Jos käyttäjien tietoja säilytetään pitkäaikaisesti, niistä voidaan myös tehdä johtopäätöksiä vielä pitkänkin ajan kuluttua sisältöjen lukemisesta.

Verkkosensuurin lyhyt historia

Verkkosensuurin kehityskulut voidaan tiivistää neljään eri jaksoon: avoimen verkon aikaan, verkon suodatuksen aikaan (”access denied”), ver-

kon kontrollin (”access controlled”) aikaan ja verkkokiistojen aikaan (”access contested”).

Avoimuuden ajanjakso kesti verkkoajan alusta 2000-luvulle. Siihen kuului idealismi verkosta uudenlaisena avoimuuden ympäristönä, joka on vapaata ja säätelemätöntä tilaa. Sensuuri ja lainsäädännölliset rajoitukset olivat käytännössäkin vähäisiä. ”Information wants to be free” –oli tämän ajan sloganeita.

Seuraavan viiden vuoden aikana kontrollin menetelmät kehittyivät ja säätely lisääntyi. 2000-luvun puolivälistä vuoteen 2010 kontrollin menetelmät kehittyivät ja hienojakoistuivat. Käyttäjiin voitiin haluttaessa puuttua täsmällisesti (”just in time”): reaaliaikaisesti ja paikannettuna. Sensuuria ja tietovalvontaa harjoittavien toimijoiden joukossa alkoi olla moninaisuutta: julkishallinnon lisäksi kontrollin toimijoiksi tulivat yritykset, jotka tuottivat teknologioita tai palveluja verkkoon.

2010 luvulla verkkosensuuri ja tietovalvonta oli jo levinnyt globaaliksi käytännöksi. Keskustelu sensuurista ja valvonnasta levisi myös julkisuuteen. Kansalaiset alkoivat olla kriittisiä jatkuvasti leviävän valvonnan ja sen mahdollisten vaikutusten suhteen. Verkon kontrollille löytyi vastaliike. Avoimuus ja oikeus tietoon politisoituivat teemoiksi, jotka nousivat esiin yllättävissä yhteyksissä. Arabikevät yhdisti kiistat verkkoon pääsystä muuhun demokratiakehitykseen.

Sensuuri on globaalia ja piiloutuu

Sananvapaus ja sensuuri verkkoaikana –hankkeessa, jossa olin tutkijana 2011-2012, tarkoituksena oli luoda yleiskäsitys verkkosensuurin tilasta. Hankkeen yhteenvetona kokosimme Kai Ekholmin kanssa verkkosensuurin kehityssuuntia 10 trendin kokonaisuudeksi. Trendit kuvaavat kehityssuuntia, jotka ovat näkyvissä verkkosensuurissa ja tietovalvonnassa.

2000-luvun aikana verkkosensuurista on tullut maailmanlaajuista ja hyväksyttyä. Vuonna 2010 sensuuri oli käytössä yli 60 maassa. Enää ei pohdita niinkään sitä, voiko sensuroida vai ei, vaan mitä sensuroitaisiin ja miten. Sensuurin laajuus ja sen seuraukset vaihtelevat kuitenkin eri maissa.

Sensuuri ja valvonta ovat laajentuneet demokraattisiin maihin ja niiden perusteluiksi ovat tulleet erityisesti turvallisuus, terrorismin uhka, rikostutkinta ja rajavalvonta. 9/11 tapahtumat toimivat merkittävänä käännekohtana ja vauhdittivat valvontajärjestelmien kehittämistä, mutta myös kiristivät myös valvontaan liittyvää lainsäädäntöä. Länsimaissa on leimallista, että valvonta alkaa olla teknologiseen infrastruktuuriin sisäänrakennettua. Sellaisena se on vaikutuksiltaan laaja-alaista, mutta käyttäjille näkymätöntä. Näin sen toimintatapoja, luonnetta ja kehityssuuntia on vaikea arvioida.

Kontrolli on monimutkaistunut

Nykyisellään verkkosensuurin ja tietovalvonnan käytännöt ovat monimutkaistuneet monesta syystä. Kontrollin harjoittaminen on hajautunut moniin käsiin: osallisina voivat olla hallinto, yritykset, turvallisuusviranomaiset tai yksityishenkilöt. Sensuurin motiivit, kohteet ja teknologiat vaihtelevat. Verkkosensuurin rajoja on myös vaikeampi määritellä, koska tietovalvonta ja sensuuri voivat yhdistyä kontrollin käytännöissä.

Käyttäjien tietoon pääsyyn verkossa voidaan puuttua kontrolloimalla sisältöjä, yhteyksiä tai palveluja. Suodatuksen lisäksi käytössä on monia muita teknologioita, joiden avulla voidaan seurata käyttäjiä tai koota heistä tietoa. Hakukoneet voivat pudottaa valikoidusti tuloksia pois tuloslistoiltaan tai estää pääsyn tietyille sivuille. Käyttäjistä kerättyjä tietoja voidaan hyödyntää myöhemmin siihen, että käyttäjien pääsy estetään haluttuihin tietoihin tai heitä valvotaan tarkemmin tai rangaistaan jo luettujen tietojen perusteella.

Puhutaan myös taloudellisesta sensuurista, millä tarkoitetaan esimerkiksi vaikuttamista tietoon pääsyyn hinnoittelulla. Internetin yhteydet, verkon sisällöt tai palvelut voivat tulla niin kalliiksi, että ne estävät tiettyjen käyttäjäryhmien verkkoon pääsyn. Toimijat voivat myös tarjota käyttäjille toimintamalleja tai sopimuksia, jotka mah-

dollistavat esimerkiksi käyttäjien tietojen omistusoikeuden tai käyttäjien seurannan. Jos palveluille ei ole markkinoilla vaihtoehtoja, käyttäjät joutuvat painostetuksi toimintamalleihin, jossa he joutuvat jakamaan itsestään enemmän tietoa kuin haluaisivat.

Arjen kriminalisointi

Sensuurin ja valvonnan kohteeksi joutumisen kynnys on madaltunut. Tiedonkeruu käyttäjien toimista suuriin tietokantoihin on antanut mahdollisuuksia erilaisiin tulkintoihin. Tietoa louhimalla käyttäjiä voidaan profiloida ja etsiä heidän joukostaan poikkeamia. Tämän kaltainen lähestymistapa johtaa siihen, että mitkä tahansa valtavirrasta poikkeavat kiinnostukset, tietosisällöt tai toimintatavat voivat joutua kyseenalaistetuksi. Samalla uhkana on myös, että kynnys sensuurille ja valvonnalle laskee.

Valvonnan näkökulmasta kansalaisten toimia tarkastellaan yhä enemmän riskipohjaisesti. Se sisältää melkoisen muutoksen tapaan tarkastella rajojen ylityksiä yhteiskunnassa. Olemme tähän saakka tottuneet pitkälle sääntöpohjaiseen ajatteluun. Se merkitsee luottamusta siihen, että toimiessani sääntöjen mukaan, tiedän myös sääntöjen ylityksen riskit ja niiden mahdollisesti tuottamat rangaistukset. Jos tiedän nopeusrajoituksen, hyväksyn myös ylinopeudesta saamani sakot.

Riskipohjainen käyttäjien toimien tarkastelu tehdään tyypillisesti kerätyn datan ja sen analysoinnin perusteella. Se on käyttäjille näkymätöntä. Käyttäjällä ei ehkä ole aavistustakaan siitä, millaisia profiileja hänestä syntyy. Ongelmallisia ovat kuitenkin lopputulokset, eli se, millaisten toimien kohteeksi joutuu. Tietovalvonnan ympäristöissä se voi vaihdella tulkitsijan ja hänen näkökulmansa mukaan ja esimerkiksi maan rajoja ylitettäessä. Se, mitä ei pidetä rangaistavana ilmaisuna kotimaassa, voi olla toisin toisen poliittisen ja uskonnollisen kulttuurin säännöistä käsin.

Big Data ja tiedonkeruun laajentuminen

Tiedonkeruu käyttäjistä verkkoympäristöstä ei ole vain laajentunut, vaan monikertaistunut. Erittäin laajoja tietovarastoja on jo tällä hetkellä julkishallinnolla eri maissa, sosiaalisen median ja hakupalvelujen suurimmilla toimijoilla (Google, Facebook) ja tiedonkeruuseen keskittyneillä yrityksillä (ChoicePoint, Axciom).

Käyttäjistä kerätään yhä enemmän tilannetietoa, joka liittyy esimerkiksi heidän asiointiinsa verkon palveluissa, hakusanoihin, käytettyihin toiminnallisuuksiin ja palveluihin ja niiden tietosisältöihin. Kun näitä tietoja kootaan yhteen suuriin tietovarastoihin, ne tarjoavat ajan mittaan massiivisen määrän analysoitavaa dataa käyttäjästä. Kaikki tiedot eivät näy käyttäjille, mutta pelkkä Facebookin aikajanan selailu tai Google-haku omalla nimellä osoittaa, että palvelujen muistissa on paljon sellaista tietoa, jonka on ehtinyt itse jo unohtaa.

Ubiikkiteknologiat tuovat tiedonkeruun kaikkialle

Ubiikkiteknologiat merkitsevät käytännössä käyttäjiin liittyvän tiedonkeruun merkittävää laajentumista, jossa mukana on tunnistuksen ja paikannuksen tuoma tarkkuus. Ubiikkiympäristön lähtökohtana on se, että tulevaisuudessa yhä suurempi osa esineistä ja ympäristöstä sisältää RFID-tunnisteen - ja sitä kautta automaattisesti kerää ja välittää tietoa sijainnistaan ja toimistaan langattomassa verkossa. Tietoa kerätään yksityiskohtaisemmin ja laajemmin kaikista arkisista toimista: viestinnästä, asioinnista, tiloissa liikkumisesta, liikenteestä, lukemisesta ja kuluttamisesta.

Ubiikkiympäristössä voidaan automaattisesti seurata jokaista sirutettua kirjaa, kirjaston laitetta ja tilaa – sekä niiden käyttöä ja käyttäjiä. Nämä käytännöt voivat tuottaa tarkempia raportteja ja tilastoja kirjaston käytöstä ja nopeuttaa aineistojen paikannusta. Jos käyttäjien seuranta kytkeytyy näihin rakenteisiin, ei voida enää puhua anonyymista kirjaston käytöstä. Käyttäjistä tulee lä-

pinäkyviä heistä tietoa keräävälle ympäristölle.

Käyttäjän tunnistus ja sen yhdistäminen käytettyihin tietosisältöihin rajaa ja sulkee tehokkaasti tiedon saatavuutta maissa, joissa esimerkiksi poliittisesti tai uskonnollisesti eri mieltä olevia jäljitetään ja rangaistaan. Tiedontarjonta on kapeutuu näissä olosuhteissa sille alueelle, jonka kyseisen maan ideologia sallii. Ja poikkeamat havaitaan tehokkaammin kuin koskaan ennen.

Kontrollin privatisoituminen

Sensuuri on historiallisesti ollut enimmäkseen hallinnon harjoittamaa. Verkkoympäristössä se on kuitenkin väistämättä hajautunut myös yksityisiin käsiin, sillä verkon teknologiat ovat suurelta osaltaan yksityisten yritysten käsissä. Jos hallinto tietyssä maassa haluaa harjoittaa verkkosensuuria, sen on toimittava yhdessä niiden yritysten kanssa, jotka tarjoavat verkkoon teknologioita.

Verkossa toimii kuitenkin hyvin monia erilaisia yrityksiä, jotka voivat omalta osaltaan olla tietovalvonnan tai sensuurin osapuolia ja sulkea tai avata tietoon pääsyä käyttäjille. Tietovirtoihin vaikuttavat esimerkiksi verkkoteknologioita tuottavat yritykset, laitteiden ja ohjelmistojen tuottajat, hakukoneyritykset ja sosiaalisen median tuottajat, tiedonkeruuseen keskittyneet yritykset, kustantajat ja markkinoinnin toimijat.

Konvergenssi ja keskittymiskehitys vahvistavat myös verkossa toimivien yritysten vaikutuksen alaa. Esimerkiksi hakukoneiden ja sosiaalisen median piirissä on vahvaa keskittymistä, mikä vähentää käyttäjien vaihtoehtoja, jos yritysten toimintamallit eivät heitä tyydytä. Yrityksien mahdollisuudet käyttää vaikutusvaltaansa voivat tosin olla sekä myönteisiä että kielteisiä – ja esimerkkejä on molemmista suunnista.

Tekijänoikeudet ja kirjastot sensoreina

Yritysten harjoittama sensuuri voi olla myös taloudellista. Se on korostunut tekijänoikeuksiin liittyvissä kiistoissa. Käytännössä verkkotilaa voidaan vallata muillakin keinoilla, kuten teknologioiden ja tiedon omistuksella ja patenteilla.

Kirjastojen kannalta tekijänoikeuksissa on monta suurta ongelmaa. Kirjastoille aiemmin myönnetyt tekijänoikeuslain poikkeukset ovat vähentymässä. Elektronisten aineistojen osalta on siirrytty sisältöjen omistamisesta käyttöoikeuksiin. Vaikka tilanteeseen on jossain määrin sopeuduttu, herättävät uudet käytännöt kysymyksiä. Mitä aineistoja kirjastoilla on tarjota 10 vuoden päästä?

Jatkuvat epäselvyydet tekijänoikeuksista hankaloittavat myös kirjastojen toimia. Digitointihankkeet ovat vaikeutuneet, koska tekijänoikeuksien suojaamien aineistojen käsittelystä tulee yksinkertaisesti liian hankalaa.

E-kirjojen lainausoikeuksissa on epäselvyyksiä. Laadukkaiden tieteellisten e-aineistojen hinnat ovat jatkuvasti nousseet, ja hinnoittelu on omiaan luomaan eroja korkeakoulujen ja oppilaitosten välille sen suhteen, kuinka tasokasta tutkimusta niiden piirissä voidaan harjoittaa.

Verkkosensuuria ja valvontaa on esitetty ns. välittäjäorganisaatioiden velvoitteeksi joidenkin lakiehdotusten puitteissa. Koska välittäjäorganisaatioiksi voidaan lukea palveluntarjoajien lisäksi myös esimerkiksi koulut ja kirjastot, lait ovat tuoneet kirjastoille epäkiitollisen roolin kontrolliverkoston toimijana. Tällaisia lakeja ovat esimerkiksi Digital Economy Act Britanniassa ja valvontakäytäntöjen laajentamista ehdotettiin myös ACTA-sopimuksessa, joka kaatui kansalaisliikkeiden laajan vastustuksen takia.

Kapenevat kansalaisoikeudet

Verkkosensuurin ja tietovalvonnan leviäminen ja niiden uudet käytännöt asemoivat uudelleen kirjaston roolia ja käyttäjien oikeuksia. Internetiin kohdistuneet idealistiset odotukset uudenlaisesta avoimuudesta ovat kirjastojen kannalta taittumassa kamppailuksi vapaasta verkkotilasta ja laadukkaista sisällöistä.

Käyttäjien näkökulmasta voidaan puhua myös tiedonsaantiin liittyvien oikeuksien kaventumisesta ja kansalaisten perusoikeuksiin liittyvistä

ongelmista. Tietovalvonta kaventaa sananvapautta ja tunnistus tekee käyttäjien toimet läpinäkyviksi. Jos tunnistettu tiedonkeruu ulottuu tiedonhakuihin, sosiaaliseen mediaan ja e-aineistojen käyttöön, käyttäjä joutuu myös pohtimaan, millaista tietoa hän voi hakea ja käyttää ja kenen kanssa hän voi olla yhteyksissä.

Jos käyttäjien toimien läpinäkyvyys ei tuntuisikaan ongelmalliselta Suomessa, voi asia olla toisin esimerkiksi Kiinassa, Saudi-Arabiassa tai Egyptissä.

Suurimpia ongelmat ovat tietysti maissa, joissa tila eri mieltä olemiselle on vähissä. Aivan ongelmatonta tietovalvonnan ja sensuurin leviäminen ei kuitenkaan ole meillekään – vaikka ne olisivat menetelmiltään käyttäjille näkymättömiä, niillä luodaan kokonaan uudenlaista kontrollin infrastruktuuria. Se voi toimia käyttäjien hyödyksi, mutta odottamattomin tavoin myös heitä vastaan.

Lisätietoa

Sananvapaus ja sensuuri verkkoaikana –hanke.
http://www.sananvapausjasensuuriverkkoaikana.com/

Lähteet

Deibert, Ronald J. & Palfrey, John G. & Rohozinski, Rafal & Zittrain, Jonathan (2011), Access contested: Towards the Fourth Phase of Cyberspace Controls. In: Access Contested: Security, Identity and Resistance in Asian cyberspace. Ed. by Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain. Cambridge; MIT Press, 2011.

Ekholm, Kai & Karhula, Päivikki (2012), Sleepwalking toward a control society? Ten Must-Know Trends. http://www.ifla.org/publications/sleepwalking-toward-a-control-society-ten-must-know-trends http://www.ifla.org/publications/sleepwalking-toward-a-control-society-ten-must-know-trends

Tietoa kirjoittajasta

Päivikki Karhula, johtava tietoasiantuntija
Eduskunnan kirjasto
Email. Paivikki.karhula@gmx.com