UNESSAKÄVELYLLÄ VALVONTAYHTEISKUNTAAN?

Kymmenen trendiä jotka meidän on tunnettava

KAI EKHOLM

Professori, Kansalliskirjaston johtaja

PÄIVIKKI KARHULA

Tutkija, johtava tietoasiantuntija, Eduskunnan kirjasto

SANANVAPAUS JA
SENSUURI
VERKKOAIKANA

Viime vuodet ovat olleet sananvapauden historiallista murrosaikaa, joka jättänyt pysyvän jäljen mediaan, viestintään, poliittiseen historiaan ja kansalaisaktivismiin.

Vaikka arabikevät on tuonut ilahduttavia merkkejä muutoksen tuulista ja sananvapauden laajenemisesta, kansainvälinen tilanne on todellisuudessa edelleen synkkä.

Joka neljäs maailman kansalainen elää sensuurin olosuhteissa. Internet-sensuuri ja tietovalvonta on hyväksytty maailmanlaajuisesti. Valvonnan periaatteita ja lähtökohtia ei enää aseteta kyseenalaiseksi, eikä niille haeta oikeutusta, vaan yhä useammin tyydytään pohtimaan, miten ja mitä voidaan valvoa. Internet-kehityksen seuraava vaihe, ubiikkiyhteiskunta, uhkaa seuraavaksi tuoda laajennetun ja reaaliaikaisen tietovalvonnan kaikkialle arkiseen ympäristöön.

Kansalliskirjaston johtaja ja FAIFE:n puheenjohtaja Kai Ekholm ja tutkija Päivikki Karhula ovat tutkineet sananvapauden ja sensuurin trendejä tuoreessa tutkimushankkeessa.

Johdanto ja seuraavat artikkelit ovat syntyneet osana suomalaista tutkimushanketta Sananvapaus ja sensuuri verkkoaikana professori Kai Ekholmin johdolla. Hanketta on tukenut Helsingin Sanomain Säätiö.

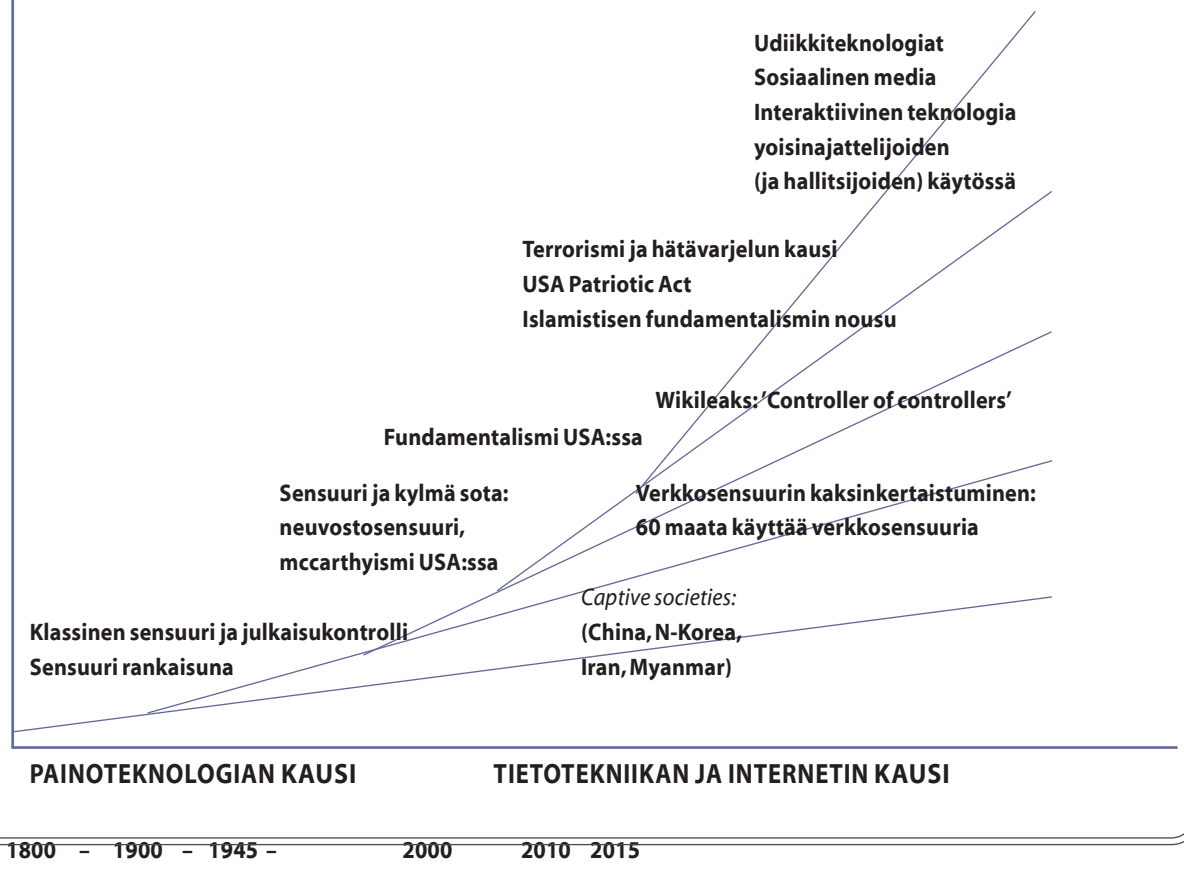
Osoitamme sydämelliset kiitokset Helsingin Sanomain Säätiölle, joka on tukenut tutkimushankettamme.
Tutkimusartikkelit edustavat kansainvälisten tutkijoiden osaamista ja antavat kuvan hankkeen tuloksista kesään 2012 mennessä. Artikkeleissa käsitellään internet-sensuurin historiaa ja sen kehityssuuntia sekä tarjotaan maakohtaisia tilannekuvauksia. Hanke jatkaa edelleen tutkimusta aiheeseen liittyvistä teemoista.

Helsinki, heinäkuussa 2012
Kai Ekholm, Päivikki Karhula

sisältö

UNESSAKÄVELYLLÄ VALVONTAYHTEISKUNTAAN?
Kymmenen trendiä jotka meidän on tunnettava

Mediamuodot ja diversiteetti



”Vapaa internet on kuollut” – valvonnasta on tullut globaalia

Valvonnan ja sensuurin rajat ovat muuttuneet internet-aikakaudella.

Internetin alkuaikoja 1990-luvulla väritti idealismi avoimesta ja vapaasta virtuaalitilasta. Sensuuria ja valvontaa ei juuri ollut. Vuosikymmenen loppuun mennessä useimmissa maissa internet oli valvonnan ja sensuurin ulkopuolella tai sitä säädeltiin hyvin kevyesti. 2000-luvun alusta lähtien kehitys kääntyi kohti jatkuvasti lisääntyvää valvontaa, joka sai seuraavalla vuosikymmenellä myös tarkentuneita ja hienojakoisempia muotoja (Deibert et al. 2011).

Sensuurista ja tietovalvonnasta on käytännössä tullut maailmanlaajuisesti hyväksyttyä. Vuonna 2010 yli 60 maassa sensuroidaan internetiä ja useissa maissa oli säädetty kansalaisten ja median sananvapautta rajoittavia lakeja (Reporters Without Borders 2010). Kansalaisiin kohdistuva valvonnan tarkkuus on myös lisääntynyt, sillä useat maat ovat asettaneet verkkoon pääsyn ehdoksi nykyisellään käyttäjien tunnistamisen, lisensoinnin tai rekisteröitymisen (Palfrey 2010). Monissa maissa myös käyttäjien mahdollisuuksia suojata viestintänsä valvontaa kryptauksella on heikennetty ja estetty (La Rue 2011).

Erilaisten valvonnan muodot ovat lisääntyneet, niiden ala on laajentunut ja niistä on tullut ominaisuuksiltaan kehittyneempiä – ja sama kehityskulku on nähtävillä sekä demokraattisissa ja autoritäärisissä maissa
(Bitso & Fourie & Bothma 2012).

Vaikka Arabi-kevät osoitti, että internetiä ja sosiaalisia verkostoja käytettiin tehokkaasti myös sananvapauden edistämiseen, autoritääriset hallitukset vastasivat aktivistien protesteihin koventamalla toimenpiteitä ja kiristämällä valvontaa. Valvonnan tila kokonaisuudessaan on synkkä - Internet-sensuuri lisääntyy yhä, mutta sitä enemmän lisääntyy tietovalvonta, josta on myös tullut yhä läpitunkevampaa (Reporters Without Borders 2012).

Internetin kontrollia toteutetaan hyvin eri tavalla eri maissa. Valvonnan syyt, käytetyt menetelmät, valvontaa harjoittavat tahot ja rangaistuksien luonne vaihtelevat laajalti. Valvonnan aikaansaamien olosuhteiden luonne vaihtelee kovien rangaistusten ja laaja-alaisista kontrolliyhteiskunnista lievempien sensuurin muotojen käyttöön maissa, joissa myös valvontaan kohdistuvaa julkista kritiikkiä sallitaan laajalti, mikä on tyypillinen länsimaisten demokratioiden käytäntö. Eroja taustoittavat oikeudelliset ja taloudelliset rakenteet ja hallinnon laatu sekä internetin infrastruktuurin tila. (Bitso & Fourie & Bothma 2012)

Tiukinta ja laajamittaisinta valvonta on tällä hetkellä Kiinassa. Kiinaa räikeänä ääriesimerkkinä käyttäen Jevgeni Morozov on osoittanut tärkeässä teoksessaan The Net Illusion (Morozov, 2011), miten diktatuurit käyttävät tehokkaasti tietoverkkoa kansalaisiaan vastaan. Kiinassa 20000 kyberpoliisia tarkkailee kansalaisten verkon käyttöä. ‘Ihmishakukoneet’ kirjaimellisesti noutavat hallituksen vastustajat kotoaan vastaamaan sanoistaan. Esimerkiksi eräs iäkäs kylänmies arvosteli verkossa hallitusta joen saastuttamisesta, ja hänet haettiin kotoa oikeuteen vastaamaan kirjoittelustaan. (Morozov 2011)

Euroopassa maat, jotka ovat viimeksi turvautuneet sensuurin laajentamiseen, ovat Unkari ja Turkki. Turkissa jokainen verkonkäyttäjä velvoitettiin käyttämään pakollista suodatinohjelmaa verkossa. Vain 22 000 maan 11,5 miljoonasta verkkokäyttäjästä on kuitenkin ottanut sen käyttöön tähän mennessä. (Reporters Without Borders 2012).

Hallitukset ovat keskeisiä internet-sensuuria harjoittavia tahoja (Bitso & Fourie & Bothma 2012). Valtaosa Internetin virtuaalisesta tilasta on kuitenkin yksityisten yritysten hallussa ja hallinnassa, mutta käytännössä eri toimijoiden vaikutukset sekoittuvat; jos hallitukset ovat halunneet laajentaa kontrollia verkossa, ne ovat usein asettaneet vaatimuksia käyttäjien seurantaan ja turvallisuusvalvontaan yksityisen sektorin toimijoille (Deibert 2012). Lisäksi

monissa valvontaa ja sensuuria edistävissä hankkeissa julkisen ja yksityisen sektorin toimijat tekevät yhteistyötä. Yksityisillä yrityksillä voi kuitenkin olla huomattavaa riippumatonta valtaa internetissä: Google, Facebook, eBay ja Amazon ovat hyviä esimerkkejä tällaisista monikansallisista yrityksistä (Hamilton & Moon 2012).

Julkisen ja yksityisen sektorin toimijoiden tai demokraattisten ja totalitääristen valtioiden väliset erot ja roolit valvonnan ja sensuurin edistäjinä eivät kuitenkaan ole selkeitä. Esimerkiksi Kiinan Suuri Palomuuri on rakennettu suurten länsimaisten ICT-yritysten, kuten Ciscon, Microsoftin, Yahoon ja Googlen tuella (BBC News 2010). Eurooppalaiset tietotekniikkayritykset ovat myyneet valvontateknologiaa ihmisoikeuksia loukkaaviin maihin kuten Egyptiin, Libyaan, Syyriaan ja Iraniin. Näitä teknologioita on käytetty kyseisissä maissa toisinajattelijoiden, ihmisoikeusaktivistien, toimittajien, opiskelijajohtajien, vähemmistöjen, ammattiliittojen johtajien ja poliittisten vastustajien toiminnan seurantaan. Niitä on voitu käyttää myös koko väestön tarkkailuun. (Privacy International 2011a)

Kaiken kaikkiaan merkittävimmät toimijat verkossa, olivatpa ne julkisia tai yksityisiä tahoja, ovat osoittaneet kykenevänsä sulkemaan tai avaamaan ovia verkkoympäristöön ja sen palveluihin, jos niin haluavat (Hamilton & Moon 2012). Se, tukevatko hallitsevien toimijoiden käytännöt pitkällä aikavälillä kansalaisyhteiskuntaa ja tiedonvälityksen vapautta, vai toimivatko näitä vastaan, on edelleen avoin kysymys - tähän mennessä poliittinen tahto on vaihdellut eri tilanteissa.

Länsimaat turvautuvat hätävarjelun liioitteluun

Länsimaisilla demokratioilla ei lähtökohtaisesti ole samoja poliittisia tai uskonnollisia syitä valvontaan kuin totalitaarisilla mailla. Länsimaissa sensuuria ja valvontaa on laajennettu muista syistä, kuten kansalliseen turvallisuuteen, terrorismin uhkaan, rikostutkintaan sekä valtion rajojen ja maahanmuuton valvontaan vedoten (Gschrey 2011, O'Brien 2010). 9/11 tapahtumien jälkimainingeissa monet valtiot ovat ottaneet käyttöön laajoja valvontajärjestelmiä ja säätäneet sodanjälkeisen ajan ankarimmat ja yksilönsuojaa rajoittavimmat lakinsa (E.g. Bloss 2007, EDRI 2011, EDRI 2012). Sananvapausjärjestöjen, kuten Privacy Internationalin ja EPIC:in (Electronic Privacy Information Center) mukaan, Yhdysvallat ja Iso-Britannia ovat kehittyneet vahvasti valvontayhteiskunniksi (Anderson 2007).

Valvonnan mekanismit rakennetaan yhä useammin internetin infrastruktuurin tasolla (Deibert et al. 2011). Vuoden 2001 jälkeen on kehitetty laajoja globaaleja, ennaltaehkäiseviä tietojärjestelmiä ja kansainvälisiä tiedonsiirtoon liittyviä määräyksiä, kuten matkustajatietojen luovutus Yhdysvalloissa ja EU:ssa (Cohen 2012, Privacy International 2004). Hallituksille on rakennettu myös ns. takaportteja verkon tietoliikenteen ja palvelujen käytön seurantaan poikkeusmenettelyjä, kuten rikostutkintaa varten. Takaportit on rakennettu osaksi verkon informaatioarkkitehtuuria, ja nämä vaatimukset on voitu perustella lainsäädännöllä ja kansainvälisillä standardeilla (esim. ETSI, Baloo 2004, Cross 2010).

Infrastruktuuriin sisäänrakennettu kontrolli on läpinäkymätöntä, mutta sen vaikutuksen ala voi olla globaali. Käytännössä nämä järjestelyt tasoittavat tietä julkisille toimijoille tai mille tahansa organisaatioille, joilla on valtaa ja intressejä päästä käsiksi verkon tietovirtoihin. Kun internetin arkkitehtuuriin on sisäänrakennettu valvontamekanismeja, niitä voidaan hyödyntää tarvittaessa julkisen tai yksityisen sektorin tarpeisiin (Hamilton & Moon 2012).

Kontrollimekanismien käyttöönottoa on tuettu myös lainsäädännöllä. Poikkeusmenettelyt ja hätätilalainsäädäntöön turvautuminen, joihin on laajalti vedottu valvonnan perusteluina, ovat viime vuosikymmenellä muuttuneet osin pysyviksi käytännöiksi. Hyvänä esimerkkinä on Patriot Act -laki USA:ssa, joka laadittiin hätätilalainsäädännöksi, mutta jonka voimassaoloa on nyt jatkettu yli 10 vuoden ajan (Goldberg 2012).

Valvonnan malleja ja perusteita myös omaksutaan herkästi maasta toiseen (Bitso & Fourier & Bothma 2012). Amerikkalaisiin valvonnan malleihin ja perusteluihin on myös syytä kiinnittää huomiota, koska ne leviävät helposti muihin maihin hallitsevien monikansallisten yritysten toimien kautta ja kansainvälisten sopimusten välityksellä. Verkon keskeiset yksityiset toimijat ovat amerikkalaisia monikansallisia yrityksiä. Kaiken kaikkiaan, USA:lla on ollut johtava rooli globaalin orientaation edistäjänä valvonnassa (Mueller 2010).

Kansalaisten laajentuva valvonta, jolla on ollut monenlaisia perusteita (esim. kansallinen turvallisuus ja copyright-lainsäädäntö) ja lainsäädännölliset muutokset ovat jo ohittaneet perusoikeuksien näkökulman, lisänneet tietovirtoihin liittyviä rajoituksia ja jättäneet huomiotta valvonnan yhteiskunnalliset vaikutukset (Carey-Smith & May 2006, EDRI 2011). USA:ssa erityisesti 9/11 tapahtumat ovat kiihdyttäneet valvontaa ja antaneet viranomaisille lisää oikeuksia etsintöihin ja takavarikkoihin (Bloss 2007).

Pelkästään teknologioilla voi kuitenkin olla kansalaisten oikeuksia kaventava vaikutus. Teknologioihin voi sisältyä erilaisia valvonnan mekanismeja, jotka on voitu rakentaa ja ottaa käyttöön ilman julkista ja poliittista keskustelua tai käyttäjien lupaa.
Jos standardit sitovat teknologian kehittäjiä rakentamaan valvontamekanismit internetin perusrakenteisiin, ne tulevat yleiseksi ja kiinteäksi osaksi verkon rakennetta. Samalla kuitenkin on

vaikea osoittaa ketään yksittäistä toimijaa Isoksi Veljeksi, joka aikoisi hyödyntää näitä välineitä omiin tarkoituksiinsa. Näin rakennettuina sensuurin mahdollisuudet piiloutuvat ja jäävät poliittisesti neutraaleiksi. Samalla myös valvonnan muodot kätkeytyvät julkiselta keskustelulta ja niistä tulee poliittisesti neutraaleja. Tämän kaltaiset teknologioiden toimintamalleihin sisältyvät kontrollin mahdollisuudet koskevat esimerkiksi sellaisia käytäntöjä, kuten takaporttien käyttöä, pakollista tunnistuskäytäntöjä, tiedonkeruuta sekä ihmisten paikantamista sekä heidän viestintänsä seurantaa.

Internetsensuurin ja tietovalvonnan monimutkaisuus

Sensuurin "klassisella" kaudella valvottiin julkaisuja tai kirjoittajia. Internetissä valvontamenetelmät eivät kohdistu vain sisältöihin, vaan ne voivat koskea käyttäjien viestintää laajemmin internetin infrastruktuurissa (La Rue 2011). Sensuurin ja tietovalvonnan menetelmiä käytetään usein myös rinnakkain. Näiden lisäksi voidaan puhua taloudellisesta sensuurista ja toimintakäytäntöjen sensuroivista vaikutuksista, kuten hinnoittelusta, pakotetusta tunnistautumisesta tai rekisteröitymisestä, internet-yhteyksien saatavilla olon säätelystä ja painostuksesta itsesensuuriin (Bitso & Fourie & Bothma 2012)

Suodatus (filtering) on tunnetuin internet-sensuurin menetelmä. Teoriassa käyttäjien rajoituksia voidaan kohdistaa

1) käyttäjän verkkoon pääsyyn,
2) käyttäjän pääsyyn tiettyyn palveluun (DNS-filtering),
3) käyttäjän pääsyyn tiettyyn sivustoon (IP-filtering),
4) käyttäjän mahdollisuuteen päästä tietylle verkkosivulle (URL-filtering) ja
5) valittujen avainsanojen jäljittämiseen perustuvaa suodatusta hyödyntämällä (keyword filtering)

(Bitso & Fourie & Bothma 2012).

On myös mahdollista yhdistää sensuuri ja tietojen valvonta. Tietovirtojen seurannalla tunnistetaan tietty ongelmallinen sisältö, jonka jälkeen sensuurin toimenpiteet voidaan kohdentaa juuri näihin löytöihin (Dutton et al. 2010).

Välittäjillä (intermediaries), kuten verkkoyhteyksien tarjoajilla (ISPs), tarkoitetaan toimijoita, jotka tarjoavat verkkoyhteyksiä tai palveluja (EDRI 2011). Verkkoyhteyksien tarjoajat voivat kontrolloida verkkoyhteyksiä teknisesti puuttumalla tietoliikenteeseen kolmella tasolla: tietoliikenteen, palvelujen tai sovellusten tai tilaajan tasolla. He voivat säädellä esimerkiksi tietoliikenteen määrää ja nopeutta. Palvelujen ja sovellusten tasolla, käyttäjiä ja sisältöjä voidaan tunnistaa tai tuottaa pääsynestoja tai joillekin sovelluksille voidaan antaa prioriteetti muihin nähden. Tilaajia voidaan rajoittaa esimerkiksi rajaamalla heidän käyttämiään kaistanleveyksiä. Yleisesti ottaen, verkkoliikenteen kontrolli näyttää olevan kohdistumassa tilaajiin yksilöinä ja siihen ollaan hyödyntämässä yksilöivän tunnistuksen teknologioita. (Finnie 2009)

Verkkoyhteyksien tarjoajilla on mahdollisuudet täydelliseen käyttäjien toimien valvontaan. Millään muulla taholla verkossa ei ole samalla tapaa niin syviä ja panoptisia näköaloja käyttäjien toimiin, koska tietoliikenteen keräämisen menetelmillä (packet sniffing) voidaan tallentaa kaikki data sähköpostiviesteistä videoihin ja Facebook päivityksiin
(Ohm 2009).

Välittäjät voivat käytännössä seurata, säännellä ja kontrolloida käyttäjien yhteyksiä, heidän palvelujen käyttöään ja heidän tuottamiaan sisältöjä. Äärimmilleen vietyjä valvonnan muotoja edustaa keskitetty, valtiojohtoinen sensuuri ja valvonta, joka on rakennettu kattamaan laajalti verkon infrastruktuuri, kuten Kiinassa. Tällainen asetelma mahdollistaa kolmentyyppisiä rajoituksia: tietoliikenteen pysäyttämistä (blackouts), tahallista yhteysnopeuksien hidastamista sekä kansallisella tasolla toteutettavaa tiedon suodatusta ja tietovalvontaa (Kelly & Cook 2011).

Tietovalvonta ja tiedonkeruu ovat sensuurin epäsuoria muotoja. Tiedonkeruu kaupallisiin tarkoituksiin on varsin laajaa, mikä jää usein huomaamatta keskimääräiseltä internetin käyttäjältä, koska tiedonkeruu on huomaamatonta ja sisäänrakennettua palvelujen normaaliin käyttöön. Esimerkiksi haku sanalla "masennus" Dictionary.com:ssa voi johtaa jopa 223 evästeen ja jäljityskuvakkeen asennukseen käyttäjien tietokoneelle, jotka mahdollistavat tiedon keruun

käyttäjistä sekä masennuslääkkeiden mainonnan kohdistamisen juuri näille käyttäjille (Etzioni 2012).

Vaikka tietovalvonnassa ei suoranaisesti estetä ihmisiä ilmaisemasta ajatuksiaan verkossa, se luo epäsuotuisat olosuhteet sananvapaudelle. Kun käyttäjien antamia tietoja voidaan koota, tallentaa ja hyödyntää muissa odottamattomissa yhteyksissä myöhemmin, tiedonkeruu voi kääntyä käyttäjien eduksi tai heitä vastaan. Siksi käyttäjien täytyy entistä tarkemmin ymmärtää verkossa viestinnän ja sen valvonnan luonne ja valita ilmaisunsa ja aiheensa huomioiden, että niistä voi olla myöhemmin seurauksia. (Etzioni 2012).

Huolestuttavinta valvonnan kehityksessä on se, että se totuttaa meidät kansalaisina valvonnan moninaisiin muotoihin.

Näin valvontayhteiskunnan kehityksen ja valvonnan kyseenalaistaminen tulee asteittain yhä vaikeammaksi.

Valvontayhteiskunnan kehitystä kuvaa hyvin ACLU:n Surveillance Society Clock (ACLU 2007).

Valvontayhteiskunnan toteuttamiselle on erittäin hyvät mahdollisuudet länsimaissakin jo nykyisellään. Tästä hyvän esimerkin tarjosi englantilainen televisio-ohjelma Erasing David. Ohjelmassa tunnettu toimittaja, David yrittää päästä valvonnan ulottumattomiin kahden yksityisetsivän jäljittäessä häntä. Eräässä kohtauksessa David on pakosalla jossakin päin Eurooppaa, kun etsivät pystyvät tuottamaan hänen kännykkänsä sijainnin perusteella tarkan kartan hänen olinpaikastaan. Davidin pako onnistuu vain muutaman päivän ajan. (Erasing David, 2010).

Arjen kriminalisointi

Valvonnan teknologioiden kehittämisen ohessa laadittu myös lainsäädäntöä, joka mahdollistaa valvonnan ja sensuurin ja madaltaa sen kynnystä; näillä laeilla on voitu kriminalisoida jopa sananvapauden laillisia alueita (La Roye 2011). Paitsi, että rikoksen määritelmiä on väljennetty ja muutettu, myös rangaistuksia rikkeistä on voitu tiukentaa (esim. tekijänoikeusrikkomuksissa, Hadopi Law).

Kansalaisten juridinen asema on jo käytännössä muuttunut. He voivat joutua helpommin epäillyksi ja joissakin tapauksissa jopa tulla pidätetyksi ilman päteviä todisteita rikoksesta, jos heitä koskevat tiedot viittaavat siihen, että heillä voisi olla yhteyksiä rikokseen. Ihmiset voidaan leimata syyllisiksi perustuen epämääräisiin todisteisiin, jotka perustuvat tietokannoista saatuun dataan – ja jää kansalaisen omalle vastuulle osoittaa, että hän on syytön (esim. tapaus Hasan Elahi, Elahi 2011). Mutta miten voisi edes olla mahdollista todistaa syyttömyytensä, jos kansalaisella ei ole käytettävissään samoja tietoja ja tietokantoja kuin viranomaisilla. Rikostutkinnan periaatteet ja menettelytavat ovat myös alkaneet olla ristiriidassa esimerkiksi monissa maissa hyväksytyn juridisen Habeas Corpus-periaatteen kanssa: ihminen tuomitaan, vasta kun hänet on todistetusti tuomittu tuomioistuimessa – hän on siis lähtökohtaisesti syytön, kunnes toisin todistetaan (Habeas Corpus).

Laajimmillaan syyllisyysperiaatteen soveltaminen heijastuu sellaisten koko väestön kattavien tietojen keräämisessä tietokannoiksi, joita on aiemmin koottu vain rikostutkintaa varten, kuten sormenjälki- ja DNA-tiedot. Useat maat ovat nopeasti lisänneet biometristen tunnistamismenetelmien käyttöä ja perustaneet tai laajentaneet biometrisia tietoja sisältäviä tietokantoja, kuten DNA- ja sormenjälkitietokantoja (Privacy International 2007).

Kriteerien madaltaminen koskee myös valvontakäytäntöjä. Ihmiset joutuvat entistä helpommin tiukemman valvonnan kohteeksi, mikä johtuu osin siitä, että käytetyt kriteerit ovat löyhentyneet, mutta myös siksi, että niistä on tullut epämääräisiä ja vaihtelevia.

Valvonnan kohteeksi joutuminen ei edellytä välttämättä yhteyttä mihinkään rikokseen, vaan jopa kansalaisaktivismi ja "epänormaali käyttäytyminen" voivat johtaa siihen, että henkilö joutuu tarkemman valvonnan kohteeksi (Dziech 2011, Johnston 2009).

Erityisesti vähemmistöihin ja marginaaliryhmiin kohdistetaan jo lisää valvontaa (Monahan 2010).

Kansalaisia kohdellaan kasvavassa määrin mahdollisena riskinä yhteiskunnalle, ja tietovalvontaa käytetään arvioimaan riskin tasoa (Heinonen 2008).

Käsite "rikoksen ennakkotutkinta" (pre-crime detection) kuvastaa hyvin kehityksen suuntaa, koska siinä keskitytään "epänormaalina" pidetyn käyttäytymisen jäljittämiseen. Mike Presdee kuvailee tällaisia käytäntöjä "arkielämän kriminalisointina", mikä puolestaan on johtamassa "kaavamaisiin ja yhtenäistettyihin käsityksiin arjesta ja ihmisten tilan katoamiseen" (Boyarsky 2002, Presdee 2000).

Massavalvonnan lisääminen, rikoskynnyksen alentaminen, voimakkaampien rangaistusten käyttö sekä näiden järjestelyjen normalisointi ja laajentaminen sen sijaan, että ne liitettäisiin poikkeusolosuhteisiin, luotaavat kehitystä kohden valvonnan kiristymistä (Saas 2012). Käytännössä näillä toimilla laillistetaan sellaisten yksilöiden ja ryhmien valvonta, joita pidetään riskinä yhteiskunnalle sekä asetetaan ensi sijalle riskien hallinta ja ohitetaan kysymykset kansalaisten perusoikeuksista ja valvonnan vastuullisuudesta ja sen käytön valvonnasta (Saas 2012). Tämänkaltaisia kehityssuuntia voidaan tunnistaa jopa joissakin läntisissä demokratioissa kuten Ranskassa ja Yhdysvalloissa (esim. Khaki 2012, Saas 2012).

Ubiikkiyhteiskunta – henkilöiden ja asioinnin laajentuva valvonta

Ubiikkiyhteiskunnassa valvonta laajentuu yksittäisten henkilöiden ja asioinnin tasolle. Perusta kaikkialle ulottuvalle valvonnalle on luotu laajamittaisella ja tehokkaalla tiedonkeruulla ja tiedonhallinnalla, jonka piiriä pyritään laajentamaan niin, että se ulottuu kaikkiin ja kaikkialle. Ubiikkiteknologia antaa välineet tunnistaa, jäljittää ja seurata ketä tahansa henkilöä tai kohdetta sekä näiden viestintää ja toimintaa. (Karhula 2012b)

Yksilöivä tunnistus on keskeinen osa ubiikki-ympäristöä. Tunnistus merkitsee myös sitä, että tunnistetiedot tyypillisesti yhdistetään kaikkiin muihin tietoihin, joita kyseisestä henkilöstä kerätään tietyssä yhteydessä. Näin henkilöä kuvaavien tietojen määrä ei vain kasva, vaan moninkertaistuu ja avaa tarkemman ja laajemman näkymän käyttäjien tietoihin.

Lopulta kaikki kerätty tieto saattaa tulla pysyvästi varastoiduksi, haettavaksi, toistettavaksi ja tiedot voidaan tarjota käyttöön tuntemattomille tahoille – ja koko prosessi on käyttäjien hallitsemattomissa (Hamilton & Moon 2012). (Karhula 2012b)

Ubiikkiyhteiskunnassa käyttäjistä tulee yhä haavoittuvampia. Heidän viestinnästään ja toiminnastaan on enemmän ja tarkemmin yksilöityä tietoa. "Big data" -käsitteellä kuvataan internetin uusia valtavia tietovarantoja. Ubiikista datasta on jo tullut laajalti kannattavaa bisnestä ja tietoa kerätään hyvin laajoihin tietokantoihin. Yhdysvalloissa ainakin 52 liittovaltion virastoa oli käynnistänyt tai käynnistämässä 199 tiedon-louhinnan hanketta, joissa hyödynnettiin yksityisten yritysten tietokantoja ja niiden tarjoamaa teknologiaa vuonna 2006 (Etzioni 2012). (Karhula 2012b)

Johtuen tietojen mahdollisesta pitkäaikais-säilytyksestä ja moninaisista käyttömahdollisuuksista henkilöön liittyvillä tiedoilla voi olla odottamattomia ja pitkäaikaisia vaikutuksia käyttäjille. Jo oman Google-tilin tarkastelu on järkytys monille tilin omistajille. Jokainen hakutoiminto tallentuu hakukoneen muistiin, vaikka se pyyhittäisiin pois omalta tietokoneelta. Yli 10 vuoden verkkohistoria yhdessä verkkopalvelussa tuottaa käyttäjästään kohtuuttoman syvän ja yksityiskohtaisen profiilin.

Automaattiset analyysit, joita sovelletaan laajalti ubiikin datan käsittelyyn, lisäävät käyttäjien riskejä. Ne luovat satunnaisia yhteyksiä ja tuovat esiin tietokannoista henkilöhistorian säröt, ristiriidat ja virheet, joka saattavat vastata käyttäjän nyky-tilannetta, mutta voi myös olla etteivät vanhat tiedot tee nykytilalle oikeutta.

Automaattiset tietojenkäsittelymenetelmät eivät anna anteeksi, eikä niillä ole myöskään huumorintajua. Jopa satunnaiset tai huumorin höystämät tiedonhaut tai tietojen selailut arkaluonteisista aiheista voivat myöhemmin tuottaa ikäviä seurauksia käyttäjälle tulemalla esiin käyttäjien profiilissa, elämäkerrassa tai heidän käyttäytymistään koskevissa ennusteissa.

Ubiikkiympäristössä kerätyt tiedot voivat rajoittaa käyttäjien toimintaa ja tulevia valintoja. Henkilökohtaisilla tiedoilla on myös käytännöllisiä seurauksia: ne voivat säädellä käyttäjien pääsyä tiloihin ja palveluihin, vaikuttaa heidän etuihinsa sekä avata tai sulkea heille tarjolle tulevia tilaisuuksia. Datan hallinnalla ja hyödyntämisellä on myös laajamittaisia vaikutuksia yhteiskunnallisiin käytäntöihin. Data ja uudet tiedonhallinnan käytännöt tuottavat uudenlaisia sosiaalisia jakoja ja rajoja ihmisten välille yhteiskunnassa (Lyon 2002). (Karhula 2012b)

Tietokantakansalaisuus - uusi kansalaisuuden muoto

Henkilöön liittyvistä tiedoista on tullut uusi valuutta, jolla on arvoa internetin seuraavan vaiheen valtataisteluissa. Google, Facebook, Amazon, eBay ja Apple sekä henkilötietoihin keskittyneet yritykset, kuten ChoicePoint ja Axciom, tekevät massiivista liiketoimintaa henkilötiedoilla. Oikeudet valtavaan määrään henkilöihin liittyviä tietoja ovat myös käytännössä kaupallisten yritysten ja hallitusten käsissä. Nämä tahot omistavat henkilöön liittyvät tiedot, voivat tehdä niillä voittoa tai luovuttaa tietoa päätöksentekoa varten.

Henkilötiedon hallitsijat ovat internetin seuraavan vaiheen uusia kuninkaita - mutta ubiikissa ympäristössä näistä tahoista tulee myös hallinnoijia, jotka voivat valvoa ja säädellä kansalaisten tietoon pääsyä, viestintää ja heidän arkisia toimintojaan. (Karhula 2012b)

Tietokantakansalaisuus on uusi kansalaisuuden muoto, jota lainsäätäjä ei tunne. Tietoja jokaisesta kansalaisesta on sadoissa rekistereissä. Kerätyn tiedon laajuuteen vaikuttavat henkilön oma aktiivisuus ja rooli, tekninen ympäristö ja yhteisöjen aktiivisuus. Kun suurin osa jokapäiväisestä toiminnasta ja palveluista liittyy jotenkin verkkopalveluihin, käyttäjien mahdollisuus säädellä tiedonkeruuta kaventuu edelleen. Tämä johtuu siitä, että seurannan käytännöt ovat suurelta osin piilotettuja ja kietoutuvat verkon tavanomaisiin toimintatapoihin, joita on vaikea välttää.

Tietosuojavaltuutettu Reijo Aarnio laati vuonna 1988 selvityksen kaikista henkilörekistereistä ja -tietokannoista Suomessa. Selvityksen mukaan Suomessa oli jo tuolloin noin miljoona eri rekisteriä tai tietokantaa (Salminen 2011). Selvitys luettelee kaikki julkishallinnon perusrekisterit ja tietokannat kuten väestörekisteri, kiinteistörekisteri, rakennus- ja huoneistorekisteri. Myös kunnilla on useita rekistereitä, mm. terveydenhuoltoon, koulutukseen ja asumiseen liittyvät rekisterit. Jokaista kansalaista koskevat myös pankkien, luottokorttiyhtiöiden, maksuhäiriöviranomaisten, kaupan yritysten, tele-operaattoreiden ja nettiyritysten rekisterit.

Virallisia tietokantoja ja rekistereitä sentään valvotaan - ja monessa läntisessä maassa suojataan jopa lainsäädännöllä.

Suomessa jokainen voi pyytää rekisteriotteen itseään koskevista tiedoista. Lain mukaan jokaisen rekisterin pitää antaa seloste sen yksityisyyspolitiikasta. Sen pitää olla saatavilla jokaiselle, joista tietoja kerätään. (The Office of the Data Protection Ombudsman)

Valitettavasti tietosuojakäytännöt eivät koske suuria monikansallisia toimijoita. Käyttäjillä ei yleensä ole pääsyä yksityisten tahojen tietokantoihin, eivätkä he pysty valvomaan heitä koskevien tietojen pätevyyttä ja käyttöä. Käyttäjät eivät myöskään kykene kontrolloimaan itse tuottamiaan tietoja. Tietojen poistaminen voi olla mahdotonta samoin kuin tietojen tulevien käyttötapojen hallinta - jopa käyttäjien oikeudet tuotettuun tietoon on voitu luovuttaa sopimuksella palveluntarjoajalle.
Käyttäjät eivät voi todellakaan luottaa siihen, että heitä koskeva tieto ja heidän tuottamansa tieto tulisi oikeudenmukaisesti käytetyksi pitkällä aikavälillä, varsinkin kun tiedot voidaan yhdistää, käsitellä ja tulkita erillään alkuperäisestä yhteydestä eri tarkoituksia varten. (Karhula 2012b)

Julkishallinnon toimetkaan eivät ole kaikilta osin läpinäkyviä. Esimerkiksi USA:ssa ilmoitettiin vuonna 2006, että kolme suurta telepalvelujen tarjoajaa, AT & T, Verizon ja BellSouth, olivat tehneet yhteistyötä NSA:n (kansallinen turvallisuuspalvelu) kanssa toimittamalla "kymmenien miljoonien amerikkalaisten" puhelimen käyttötiedot - ohjelma, jota on kuvattu "maailman tähän asti suurimmaksi tietokannaksi". (Etzioni 2012)

Kuulemme mielellään lisää eri maiden tietosuojakäytännöistä.

Internetin valvonnan yksityistäminen

Sähköisen tilan valtaus on osa laajenevaa verkkokapitalismia – ja siihen on liittynyt verkkoaikana jatkuvia valtataisteluja keskeisten toimijoiden kesken Internetissä (Manjikian McEvoy 2010). Internetin kaudella tiedon hallinnoijiksi on syntynyt monia erilaisia tahoja: verkkoteknologioiden tuottajia, laitteisto- ja ohjelmistotoimittajia, hakukoneyrityksiä, sosiaalisen median yrityksiä, datan ja sisältöjen tuottajia ja markkinointiyrityksiä. Näiden uusien sidosryhmien kasvava vaikutus perustuu myös ilmeiseen konvergenssin trendiin, joka on internet aikana toteutunut sisältöjen, median ja erilaisten verkkoon liittyvien teknologioiden yhdentymisenä, mutta myös kaupallisten yritysten tehokkuutta lisäävinä yhteensulautumisina.

Kaikki edellä mainitut osapuolet, kustantajien ja tiedotusvälineiden ohella, voivat säädellä käyttäjien tietoon pääsyä. Kuitenkin yritysten kapasiteetti on ylittänyt internet-sensuurin aiempien vaiheiden mittasuhteet: nämä osapuolet voivat paitsi säädellä sisältöjä myös hallita viestintää ja tietovirtoja tai tarkkailla käyttäjien toimintaa ja viestintää tietovalvonnan avulla ja säädellä pääsyä henkilöihin liittyviin tietoihin. Hallitukset ovat myös ottaneet huomioon näiden tahojen mahdollistaman valvonnan; Euroopassa ja USA:ssa hallitukset ovat yhä enemmän painostaneet välittäjiä ja verkkoyhteyksien tarjoajia suoraan tai epäsuoraan verkkoliikenteen valvontaan ja seurantaan monista syistä lähtien verkon teknisen toimivuuden takaamisesta tekijänoikeusrikkomusten valvontaan (EDRI 2011).

Yksityisten yritysten keskeinen rooli valvonnassa mahdollistaa myös taloudellisen sensuurin. Hallitsevat yritykset voivat yrittää vallata markkinat, vaikuttaa sopimusehtoihin ja toimintamalleihin; tai ne voivat vaikuttaa käyttäjien oikeuksiin määrittelemällä, missä määrin käyttäjät voivat hallita tietojaan tai säännellä tietovirtojaan. Nämä uhkakuvat eivät ole vain filosofisia, sillä esimerkiksi Applea syytetään parhaillaan e-kirjakartellista - ja internetin merkittävien toimijoiden välillä on jatkuva valtataistelu (Whittaker 2012).

Määräävä markkina-asema on vaikuttanut myös liiketoimintamalleihin, kuten jakelupolitiikkaan. E-lehtiä voidaan myydä kalliina lehtipaketteina, ilman että muita vaihtoehtoja olisi tarjolla. Artikkelien saatavuus voidaan taata vain tietyksi ajaksi ja sen jälkeen jo maksetut numerot voidaan vetää pois käytöstä (McDermomtt 2012). Kaiken kaikkiaan tieteellisen tiedon hinta on jatkuvasti noussut, mikä uhkaa jo tutkijoiden ja oppilaitosten ja korkeakoulujen tiedonsaantia (Panitch & Machalak 2005, White & Creaser 2007). Kalliisiin tietokantoihin ei ole enää jokaisessa yliopistossa varaa. Kun tiedonsaanti rajautuu tiedon hinnan vuoksi, laadukas tutkimus voi eriytyä eliittiyliopistoihin ja oppilaitoksiin madaltaen oppimisen ja tutkimuksen laatua muissa oppilaitoksissa (Lessig 2011).

Kaupan keskittymis- ja konvergenssikehitys vaikuttaa epäedullisesti myös kuluttajiin ja välittäjäorganisaatioihin kuten kirjastoihin. Vaihtoehtoiset sisällöt vähenevät ja neuvottelun mahdollisuudet pienenevät. Suurten toimijoiden lakimiehet panevat pienemmät yksittäiset toimijat ahtaalle.

Kiristyneet tekijänoikeudet ja patenttilait kaventavat pääsyä tietoon

Tiedon kulkua ja tiedon käyttöä on viime aikoina rajoitettu ja säädelty erityisesti tekijänoikeuslainsäädännöllä. Yritykset käyttävät myös patentteja riistääkseen muilta käyttäjiltä virtuaalisen tilan (Gustin 2012). Patentointi voi lopulta uhata tieteen tulevaisuutta.

Käyttäjille tekijänoikeusrajoitukset näyttäytyvät yhä suhteettoman kovina toimenpiteinä, kuten teosten kohtuuttoman pitkinä suoja-aikoina. Pitkät suoja-ajat estävät julkaisujen digitoinnin verkkoon yleistä käyttöä varten esim. kirjastoissa ja museoissa (McDermott 2012). Käytännössä kaikki 1900-luvun tärkein aineisto on kaupallisesti suojattua siitä huolimatta, että nämä asiakirjat eivät ole välttämättä saatavilla edes kirjakaupoista. On paradoksaalista, että nykytilanne ei oikeastaan tuo voittoja kenellekään. Eikä pitkä suoja-aika noudata julkaisujen kierron syklejä ja niiden käytön paradigmoja.

Kirjastoille ja museoille myönnetyt poikkeussäännökset ovat myös vähentymässä. Tämä merkitsee uusia esteitä kansalaisten tiedonsaannille tulevaisuudessa. Yleiset kirjastot käyvät ankaraa kamppailua e-kirjojen lainausoikeuksista (Coffman 2012). Ilman mahdollisuutta lainata e-kirjoja ne jäävät armotta verkkokehityksen ulkopuolelle. Tekijänoikeudet aiheuttavat kirjastoille myös käytännön ongelmia, joihin ei ole helppoja ratkaisuja. Kuka tietää, ketkä ovat 1930-luvun sanomalehtien oikeat oikeudenomistajat? Miksi vanhoja lehtiä ei voi tuoda vapaasti verkkoon kohtuullista korvausta vastaan?

Omistusoikeuksista on siirrytty käyttöoikeuksiin. Parhaimmillaankin käyttäjä, kuten kirjasto, voi lainata tai lisensoida julkaisun käyttöönsä joksikin aikaa (McDermott 2012). Jos sama julkaisu on myöhemmin tarpeen, se on hankittava uudelleen. Nämä käytännöt synnyttävät uudenlaisia pelkoja. Onko julkaisua enää edes olemassa markkinoilla 10 vuoden päästä muodossa, jossa se voidaan lukea? Mitä julkaisuja kirjastoissa on 10 vuoden päästä?

Nämä näkökulmat tuovat aivan uusia kysymyksiä tiedonsaannin rajoituksiin.

Virtuaalisesta tilasta taistellaan jatkuvasti: kuka omistaa sen ja kuka säätelee sitä? Kenellä ovat oikeudet sen sisältöihin ja kuka saa niistä voittoa?

Kuten Hamilton ja Moon ovat osoittaneet, nyt on aika vaikuttaa tähän kehitykseen. Tekijänoikeuslainsäädäntö on edelleen muutoksessa. Tulevaisuus näyttää, tuleeko internetin rakenteista joustavia vai tukevatko tekijänoikeuslainsäädännön muutokset vanhoja malleja ja teollisuuden lobbareiden etuja (Hamilton & Moon 2012).

Valvonnan rooli siirtyy välittäjille

Kehityksen suunta osoittaa, että hallitukset ovat lisääntyvässä määrin painostaneet Internetin välittäjiä ottamaan kontrolloijan roolin ja tutkimaan, seuraamaan ja rankaisemaan käyttäjiä. Käyttäjiä seurataan ja heidän toimiaan verkossa tallennetaan, heidän pääsyään rajoitetaan ja estetään ja heitä rangaistaan. Välittäjät ovat varuillaan omasta puolestaan, koska ovat laillisten velvoitteiden alaisia käyttäjien toimista. Kehityssuuntaus on näkyvillä Euroopassa ja USA:ssa. (EDRI 2011)

Tekijänoikeuslainsäädäntö on nostanut esiin muitakin tiedonvapauden rajoituksia. Viime vuosina esitetyt ehdotukset ovat kattaneet sellaisten valvontamekanismien toteuttamisen, joilla jäljitetään lisensoitujen materiaalien laittomat kappaleet. Velvoitteita tällaisiin käytäntöihin ovat osoittaneet esimerkiksi ACTA-sopimus, brittiläinen Digital Economy Act ja ranskalainen Hadopi –laki (ACTA, Digital Economy Act, EDRI 2011, Hadopi Law).

Huolestuttavinta näissä järjestelyissä on, että ne luovat käytäntöjä, joilla seurataan kaikkia käyttäjien tietoja tekijänoikeuskysymyksen varjolla ohittaen samalla käyttäjien yksityisyyden rajat.

Jos nämä käytännöt jäävät pysyviksi, ne voivat synnyttää kontrollin rakenteet, joita voidaan myöhemmin käyttää muihin tarkoituksiin – ja laajentaa näin tietovalvonnan ja sensuurin alaa.

Tekijänoikeuslainsäädäntöön liittyvät toimenpiteet ja kansainväliset sopimukset ovat asettaneet uusia valvontavelvoitteita verkkotiedon välittäjinä toimiville tahoille. Nämä järjestelyt voivat myös velvoittaa sellaisia toimijoita, kuten hotellit, kahvilat, yliopistot ja kirjastot ottamaan vastuun lisensoimattoman materiaalin käytön valvonnasta. (Hamilton & Moon 2012)

Myös tekijänoikeusloukkauksista annetut rangaistukset ovat koventuneet. Esimerkiksi Digital Economy -laki Iso-Britanniassa ja Hadopi-laki Ranskassa soveltavat niin sanottua "kolmen iskun" periaatetta (Digital Economy Act, Hadopi Law). Jos nuori perheenjäsen rikkoo lakia kolmesti, pääsy internetiin voidaan evätä koko perheeltä. Jos kirjasto rikkoo lakia kolme kertaa, sen internet-yhteys voidaan katkaista.

Kansalaisjärjestöt ja välittäjäorganisaatiot, kuten kirjastot, ovat nousseet vastarintaan vastustaakseen viimeaikaisia päätöksiä tarkkailla ja valvoa kansalaisten tiedonkäyttöä (esim. osana Digital Economy Act -säädöstä Iso-Britanniassa ja ACTA-sopimuksen yhteydessä) (Du Preez 2011, IFLA 2011, IFLA & EBLIDA 2012).

Kansalaisoikeuksien ja demokratian haaste

Sähköisten kansalaisoikeuksien perusoikeus on vapaa tiedonsaanti ja vapaa tietojen käyttö ilman uhkaa yksityisyydelle. Nämä edellytykset eivät enää täyty.

Sensuuri ja tietovalvonta ovat laajentuneet maailmanlaajuisiksi käytännöiksi. Hallitukset säätävät yhä useammin lakeja tai muuttavat voimassaolevia lakeja laajentaakseen valtaansa kansalaisiin päin ja tarkkaillakseen internetin käyttäjien toimintaa ja viestintää ilman, että kansalaisilla olisi riittävät takeet siitä, että tietoja ei väärinkäytetä. (La Rue 2011)

Myös kysymykset käyttäjien oikeuksista ja sensuurista ovat tulleet monimutkaisemmiksi: enää ei ole kysymys vain käyttäjien pääsystä tietoihin. Kontrollimekanismit internetissä voivat puuttua sisältöihin, tietoon pääsyyn, tietoliikenteeseen, jakeluun, laajemmin internetin infrastruktuuriin tai vaikuttaa suoraan käyttäjiin tai jakelijoihin – ja tietovalvontaa ja sensuuria voidaan yhdistellä näissä lähestymistavoissa.

Pääsy internetiin ja sisältöihin eivät yksinään takaa, että viestintä olisi verkossa käyttäjille turvallista. Jopa tiukasti vartioidut kiinalaiset pääsevät verkkoon ja he voivat kirjoittaa blogeja ja käyttää paikallisia sosiaalisen median palvelujakin. Kuitenkin huomattava määrä tietoa ja keskeisiä palveluja on suodatettu pois heidän käytöstään, ja kiinalaisten on oltava hyvin varovaisia ilmaisuvapautensa kanssa ja ennakoitava viestiensä seuraukset.

Kaiken kaikkiaan, kontrollin mekanismit ovat laajalti vallanneet virtuaalisen tilan ilman, että olisi käyty julkista keskustelua siitä, miten valvonnan lähtökohtaisesta hyväksyttävyydestä ja sen yhteiskunnallisista vaikutuksista tai siitä, miten valvojia valvotaan. Laajempi ymmärrys ja julkinen keskustelu valvontamekanismien olemassaolosta, niiden ulottuvuuksista ja vaikutuksista ollaankin käymässä vasta, kun valvontajärjestelmät ovat jo käyttöön otettuja. Kansalaiset eivät välttämättä edes tiedä sitä, millainen käytös verkossa tulkitaan epäilyttäväksi tai rikolliseksi, koska näiden käsitteiden tulkinta on nopeasti muuttunut ja tullut epämääräiseksi.

Ubiikkiyhteiskunnan kehittäjät puhuvat avoimuuden lisäämisestä. Tämä on perustavanlaatuinen väärinkäsitys. Ubiikkiympäristö tukee pääasiassa yksisuuntaista avoimuutta: käyttäjistä tulee läpinäkyvämpiä tietojen hallinnoijille ja omistajille. Läpinäkyvyys ei kuitenkaan ole vastavuoroista. Näin käyttäjät ovat entistä alttiimpia heitä koskevien tietojen väärinkäytölle ja heistä tulee ensisijassa tiedonkeruun ja valvonnan kohteita. Ubiikkiympäristö tarkoittaa käytännössä ihmisten ja ympäristön hallittavuuden kasvua, joka näyttää hyödyttävän eniten tiedonhallinnoijia ja omistajia, mutta jättää käyttäjät tiedonkeruun kohteiksi ja avaa heille rajattuja näkymiä ja palveluja, jotka perustuvat heistä kerättyihin tietoihin. (Karhula 2012b)

Läpinäkyvyys ja yksityisyys ovat keskeisiä huolenaiheita valvontajärjestelmien levittäytyessä. Sinänsä yksityisyyden ja läpinäkyvyyden periaatteet tukevat ja täydentävät toisiaan periaatteet oikeusvaltion ja demokraattisen yhteiskunnan ylläpitäjinä.

Yksityisyys on tärkeää kansalaisille, koska muut kansalaisoikeudet, kuten sananvapaus, mielipiteen vapaus, uskonnon vapaus tai yhdistymis- ja liikkumisvapaus, eivät voi toteutua ilman yksityisyyttä.

Tiedollinen yksityisyys (informational privacy), joka soveltuu tarkemmin myös verkossa viestimisen rajojen kuvaamiseen, määrittelee yksilölle rajoja ja suojia valtion hänen toimiinsa puuttumista vastaan (Bannister 2005). Yksityisyys siis käsitteenä määrittelee kansalaisen tilaa, jossa hän voi määrätä olemisestaan ja tekemisistään itse muiden puuttumatta asiaintilaan. Verkossa asetelma on kuitenkin monimutkaisempi, koska kommunikaatioon ei puutu vain valtio, vaan yksityisyyden rajoja voita ylittää myös yksityiset yritykset, organisaatiot tai muut kansalaiset.

Kaiken kaikkiaan, tiedollinen yksityisyys kuvaa tässäkin kontekstissa hyvin käsitteenä yksilön oikeutta määrittää omaan tilaan, sen rajoihin ja itsemääräämisoikeuteen.

Julkishallinnon ja poliittisen vallankäytön avoimuus ja läpinäkyvyys ovat perinteisiä toimivan demokratian merkkejä (Firmino 2010). Läpinäkyvyys on periaate, jota on tarkoitus soveltaa julkisen vallan toimijoihin ja muihin organisaatioihin, joilla on merkittävää valtaa yhteiskunnassa niiden vastuullisuuden ja hyväksyttävän toiminnan takaamiseksi. Näin syntyy tasapainottava mekanismi yhteiskunnalliselle vallankäytölle ja sen valvonnalle.

Nykykehityksen paradoksi on, että kansalaisoikeuksien perustaa on rapautumassa yksityisyyden kapenemisen ja anonyymiyden vähentämisen takia. Samalla lisätään läpinäkyvyyttä väärään suuntaan – kansalaisten toimet tulevat yhä läpinäkyvämmiksi ja hallittavimmiksi niille tahoille, jotka hallitsevat heidän tietojaan. Läpinäkyvyyden oikealla käytöllä voitaisiin tehostaa hallinnon laatua ja vaikutusvaltaisten toimijoiden valvontaa yhteiskunnassa. Verkossa hallitsevien toimijoiden avoimuus on kuitenkin vähentymässä ja niiden toimien kontrolloimattomuus lisääntymässä. Kehitys vahvistaa hallitsevien toimijoiden valtaa kansalaisiin jo lähtökohtaisesti siksi, koska heillä on käytössään erittäin tehokkaat massojen hallinnan välineet. (Karhula 2012b)

Kansalaisten oikeuksien ja demokratian periaatteiden rapautuminen on väistämätön seuraus, kun laaja-alaisia kontrollimekanismeja otetaan käyttöön ja niiden käyttöönotossa toistuvasti ohitetaan kansalaisoikeuksien suojaamisen edellyttämät toimet. Demokratian ja kansalaisoikeuksien nykytila olisivat kuitenkin edelleen ajankohtaisia kysymyksiä tutkimukselle ja julkiselle keskustelulle.

Mikä on demokratian laatu ja tila nykyisellään? Miten voitaisiin löytää vallan tasapaino kansalaisten, julkisen ja yksityisen sektorin ja muiden keskeisten verkossa toimijoiden kesken? Miten perusoikeudet verkossa voitaisiin turvata?

Kaiken kaikkiaan, käyttäjin oikeuksia verkossa tulisi katsoa verkkoon ja sisältöihin pääsyä laajemmin niin, että ymmärretään, että sananvapauden ja sensuurin kysymykset ja kontrollin menetelmät ovat laaja-alaisempia: ne liittyvät laajemmin internetin infrastruktuuriin. Laajemmassa kontekstissa käyttäjillä pitäisi olla oikeuksia myös erilaisiin mielipiteisiin ja erilaisten sisältöjen tuottamiseen ilman pelkoa. Käyttäjillä tulisi myös olla laajemmin oikeuksia heihin liittyviin tietoihin, kuten oikeus tarkistaa ja korjata heihin liittyvät tiedot ja seurata, kuinka heihin liittyvää tietoa käytetään (esim. EU:n tietosuojalainsäädäntö tunnistaa nämä vaatimukset ja ne kuuluvat käsitteeseen data subject rights, EDPS 2012).

Suljettu ja läpinäkymätön verkon infrastruktuuri, johon sensuuri ja valvonta asettuvat, tulisi avata tulevaisuudessa. Tiedonkeruu ja tiedonhallinta piiloutuvat yhä enemmän käyttäjiltä. Siinä kontekstissa käyttäjät tarvitsisivat yhä enemmän myös tietoa siitä, millainen on valvonnan konteksti ja rakenne laajemmin ja miten heidän tietojaan käytetään siinä (Clarke 2007). Ympäristössä, jossa kerätään koko ajan lisää tietoa, käyttäjät tarvitsisivat myös lisää menetelmiä, jotka suojaisivat heitä liialliselta seurannalta, valvonnalta ja heidän tietojensa käytöltä ilman heidän lupaansa. Muutoin ubiikkiyhteiskunta tulee kaventamaan kohtalokkaalla tavalla kansalaisoikeuksia.

Johtopäätökset

Internet-sisältöjen ja -viestinnän valvonta on lisääntynyt huomattavasti 2000-luvun alusta tähän päivään. Se näkyy teknologioissa, laeissa ja yhteiskunnallisissa käytännöissä. Näiden kehityskulkujen yhdistetty vaikutus on siinä, että ne ovat synnyttäneet edellytykset laajamittaisille valvontamekanismeille, niiden juridisille perusteluille ja kansalaisoikeuksien uudenlaisille tulkinnoille.

Internet-sensuuri ja tietojen valvonta ei aina merkitse välittömiä rajoituksia, mutta tietojen mahdollinen moninainen jatkokäyttö uhkaa käyttäjiä myös länsimaisissa demokratioissa. Laajamittaisen tiedonkeruun oloissa ihmiset käytännössä painostetaan mukautumaan tähän kehitykseen, jos he haluavat suojella etujaan ja varmistaa, että tilaisuuksien ovet avautuvat heille tulevaisuudessa.

Jos valvonnan ja sensuurin käytännöt yhä tiukentuvat, ne voivat jäädyttää julkisen keskustelun ja aiheuttaa turvattomuutta ja pelkoa viestinnässä. Uudet valvontamekanismit uhkaavat kaikkien vähemmistöjen etuja sekä sellaisia yksilöitä ja ryhmiä yhteiskunnassa, joilla on poikkeava näkemyksiä tai elämäntapoja.
(Etzioni 2012, Karhula 2012b)

Vakavimmat seuraukset nykykehityksestä kohdistuvat kansalaisiin, jotka elävät totalitaarisissa maissa, joissa voidaan langettaa vakavia rangaistuksia vastustavista mielenilmauksista (La Rue 2011). Samat valvonnan käytännöt, kuten käyttäjien pakollinen tunnistautuminen ja tietovalvonta, jotka voivat olla perusteltuja tietyissä yhteyksissä länsimaisissa demokratioissa, tekevät elämästä hengenvaarallista yhteiskunnissa, joissa poliittinen ilmapiiri on erilainen. Lisäksi ei ole takeita, että demokraattinen tasapaino länsimaissa tulee olemaan pysyvä pitkällä aikavälillä.

Nämä samat seuraukset voivat uhata tiedostusvälineiden ja kansalaisten suhdetta, koska on olemassa merkkejä lähdesuojaa ja käyttäjien anonymiteettiä uhkaavasta politiikasta. Toimittajat kuuluvat kohderyhmään, jota valvotaan tiukemmin myös Euroopan maissa (Privacy International 2011b). Myös kiristynyt kilpailu media-alalla estää yrityksiä valvomasta käyttäjien viestintää tarkemmin, mikä puolestaan asettaa taas käyttäjät lisääntyvän tietovalvonnan kohteiksi (Turow 2011).

Lähdesuoja ei koske pelkästään mediaa, vaan se tukee myös demokratian rakenteita yhteiskunnassa. Huolimattomuuksia tai väärinkäytöksiä esiin tuovat vuodot (whistle-blowing) on hyväksytty vallan tasapainoa ylläpitäväksi etukäteisvaroitusjärjestelmäksi ja tehokkaaksi välineeksi taistella korruptiota, petoksia ja huonoa hallintoa vastaan. Vuotojen tärkeys on tunnustettu myös kansainvälisesti YK:n ja OECD:n taholta (Osterhaus & Fagan 2009).

Jos lähdesuoja rapautuu, myös tärkeä osa demokraattisen yhteiskunnan vallan tasapainon takaamista ja hallinnon vastuullisuuteen ja hyväksyttävyyteen kohdistuvaa valvontaa tuhoutuu.

Internetin hallitsevilla toimijoilla on yhä enemmän valtaa. Ne voisivat kuitenkin käyttää merkittävää valtaansa tuottamalla laaja-alaisia myönteisiä vaikutuksia, jotka tukisivat kansalaisoikeuksia ja demokratiaa. Poliittinen paine, kuluttajien ja aktivistien toiminta ovat joissakin tapauksissa saaneetkin yritykset muuttamaan politiikkaansa ja osoittamaan, että he pystyvät halutessaan tekemään myös eettisiä päätöksiä. Esimerkiksi Google ilmoitti vuonna 2010, että se lopettaa sensuurin harjoittamisen yrityksen hakupalvelujen kiinalaisessa versiossa (Fay 2010, Reporters Without Borders 2010).

Yritykset voisivat toimia valvonnan ja sensuurin vastavoimina ja avata uusia mahdollisuuksia käyttäjien oikeuksien suojalle. Näin voitaisiin tuoda tasapainoa käyttäjien oikeudelliseen asemaan ja tarjota käyttäjille toiminnallisuuksia, joiden avulla käyttäjät voisivat suojella yksityisyyttään, hyödyntää anonyymiyttä tai valvoa omia tietojaan tai rajata heihin kohdistettavaa seurantaa ja paikantamista. Hyviä esimerkkejä sensuurinvastaisista toimista on myös lainsäädännössä,

kuten Do Not Track –käytäntö, Net Neutrality –hankkeet ja islantilainen IMMI-lainsäädäntö, johon pyritään kokoamaan parhaat osat tiedollisia oikeuksia ja sananvapautta tukevista käytännöistä. (Hastings 2011, Howe & Nissenbaum 2008, IMMI Status report 2012, Pike 2011, Wu 2007).

Sensuuri ei ole uusi ilmiö. Internet-sensuuri on kuitenkin luonteeltaan ongelmallisempi ja voimakkaampi, koska sen vaikutusten ala voi olla verkossa globaali; se mahdollistaa sellaisia massavalvonnan muotoja, joille ei ole mitään vertailukohtaa aiemmissa sensuurin muodoissa (Bitso & Fourie & Bothma 2012). Kaiken kaikkiaan jokainen tehokas laaja-alainen valvontajärjestelmä, jollainen myös ubiikkiyhteiskunta on, tuo mukanaan huomattavia riskejä demokraattiselle yhteiskunnalle ja kansalaisoikeuksille.

Koska laaja-alaisia valvontajärjestelmiä on jo otettu käyttöön tai uusien järjestelmien käyttöönotto on etenemässä, olisi vakavasti tarpeen huomioida niiden rajoitukset ja seuraukset kansalaisille.

Valvonnan kehityskulut olisi tunnistettava, ymmärrettävä ja sen vaikutuksia olisi arvioitava. Poliittisessa päätöksenteossa olisi tärkeää puuttua säätelyn keinoin massojen valvontaan ja sen välineisiin sekä varmistaa niiden vastuullinen käyttö siten, että demokratia ja kansalaisoikeudet pysyvät edelleen voimassa.

References

ACLU (2007). Surveillance Society Clock. 4.9.2007. http://www.aclu.org/technology-and-liberty/why-surveillance-society-clock

ACTA. Anti-Counterfeiting Trade Agreement http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement

Anderson, Nate (2007), US and UK have become "endemic" surveillance societies. ARStechnica.com, 31.12.2007. http://arstechnica.com/uncategorized/2007/12/us-and-uk-have-become-endemic-surveillance-societies/

Baloo, Jaya, ETSI & Lawful Interception of IP-traffic. RIPE-48 Meeting, May 2004. http://meetings.ripe.net/ripe-48/presentations/ripe48-eof-etsi.pdf

Bannister, Frank (2005), The panoptic state: Privacy, surveillance and the balance of risk. Information Polity 10 (2005): 65–78.

BBC News (2010), Timeline: China and net censorship. Last update: 23 March 2010. http://news.bbc.co.uk/2/hi/8460129.stm

Bitso, Constance & Fourie, Ina & Bothma, Theo (2012), Trends in transition from classical censorship to Internet censorship: selected country overviews. FAIFE Spotlight, 2012. http://www.ifla.org/faife/spotlight

Bloss, William (2003), Escalating U.S. Police Surveillance after 9/11: and Examination of Causes and Effects. Surveillance & Society, Part 1, 4(3):2007. p208-228.

Boyarsky, Nicholas (2002), The Technique of Space. In: Leon Van Schaik & Peter Lyssiotis, Poetics in Architecture: 82-83. London; New York: Architectural Design; Wiley Academy, 2002.

Carey-Smith, Mark and May, Lauren (2006) The Impact of Information Security

Technologies Upon Society. In: Proceedings Social Change in the 21st Century

Conference 2006, Queensland University of Technology. http://eprints.qut.edu.au/6082/1/6082.pdf

Clarke, Roger (2007), What is Überveillance? (And What Should Be Done About It?)' IEEE Technology and Society 29, 2 (Summer 2010) 17-25

Coffman, Steve (2012), The Decline and Fall of the Library Empire. Searcher. April 2012, Vol 20 Issue 3. p14-47. 13p.

Cohen, Amon (2012), European Parliament Approves U.S. PNR Data Transfer Deal. BusinessTravellerNews.com. 19.4.2012. http://www.businesstravelnews.com/Worldwide-Travel/European-Parliament-Approves-U-S--PNR-Data-Transfer-Deal/?ida=Airlines&a=trans

Cross, Tom (2010), Exploiting Lawful Intercept to Wiretap the Internet. Black Hat Technical Security Conference, Jan 2010. http://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-LawfulI-Intercept-slides.pdf

Deibert, Ron (2012), Cyber Security. In: Evolving Transnational Threats and Border Security. A New Research Agenda. Christian Leuprecht & Todd Hataley & Kim Richard Nossal.(Ed.). Centre for International and Defence Policy, Queens University, Canada. http://www.queensu.ca/cidp/index/Martello37E.pdf

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.

Digital Economy Act 2010. Wikipedia. http://en.wikipedia.org/wiki/Digital_Economy_Act_2010

Du Preez, Derek (2011), Digital Economy Act threatens library internet services. Computing.co.uk, 4.2.2012. http://www.computing.co.uk/ctg/news/2024169/digital-economy-act-threatens-library-internet-services#ixzz21vUhMyq7

Dutton, William H. & Dopatka, Anna & Hills, Michael & Law, Ginette & Nash, Victoria (2010), Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet. Oxford Internet Institute, University of Oxford. A report prepared for UNESCO's Division for Freedom of Expression, Democracy and Peace. http://www.ifap.ru/library/book478.pdf

Dziech, Andrzej (2011). INDECT: Intelligent information

system supporting observation, searching and detection for security of citizens in urban environment. Presentation. 10.4.2011. http://www.indect-project.eu/files/public-stories/presentation-at-the-hq-of-polish-police/INDECT_Dziech_EN.pdf

EDPS (2012), European Data Protection Supervisor. The data subjects' rights. Page last modified: 29. heinäkuuta 2012 13:20:35. http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/QA5

EDRI (2011), The slide from "self-regulation" to corporate censorship. Discussion paper prepared by Joe McNamee. http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf

EDRI (2012), EU Surveillance: A summary of current EU surveillance and security measures. http://www.edri.org/files/2012EDRiPapers/eusurveillance.pdf

Elahi, Hasan (2011), You Want to Track Me? Here You Go, F.B.I. New York Times, 29.10.2011. http://www.nytimes.com/2011/10/30/opinion/sunday/giving-the-fbi-what-it-wants.html?pagewanted=all

Erasing David (2010). A documentary about privacy, surveillance and the database state. http://erasingdavid.com/

Etzioni, Amitai (2012), The Privacy Merchants: What Is To Be Done? University of Pennsylvania Journal of Constitutional Law 14.4 (March 2012) p. 929-951 http://icps.gwu.edu/files/2010/10/privacy-merchants.pdf

Fay, Joe (2010), Google leaves censorship to China's experts: China crisis not exactly a human rights triumph. The Register. 13.1.2010. http://www.theregister.co.uk/2010/01/13/google_china1/

Finnie, Graham (2009), ISP Traffic Management Technologies: The State of the Art. Heavy Reading. Report for the CRTC.

Firmino, Sandra (2010), Corruption and quality of democracy. 3rd ECPR Graduate Conference. 30.8.-1.9.2010. Dublin. http://www.ecprnet.eu/databases/conferences/papers/878.pdf

Gindin, Susan E. (1997), Lost and found in cyberspace. Informational Privacy in the age of the Internet. http://www.info-law.com/lost.html

Goldberg, Beverly (2012), Patriot Act Renewal Renews Reformers' Determination. American Libraries, 31.5.2012. http://americanlibrariesmagazine.org/news/05302011/patriot-act-renewal-renews-reformers-determination

Gschrey, Raul (2011), Borderlines, Surveillance, Identification and Artistic Explorations along European Borders. Surveillance & Society, Vol 9, No 1/2 (2011). http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/borderlines/borderlines

Gustin, Sam (2012). Patent Wars. Time, 23.4.2012. Vol. 179 Issue 16.

Habeas corpus. Wikipedia. http://en.wikipedia.org/wiki/Habeas_corpus

Hadopi law. Wikipedia. http://en.wikipedia.org/wiki/HADOPI_law

Hamilton, Stuart & Moon, Darren (2012), The Struggle to Scale: Keeping Up With the Internet. FAIFE Spotlight, 2012. http://www.ifla.org/faife/spotlight

Hastings, Peter (2011), "Do not track or right on track? – The privacy implications of online behavioural advertising". Public Lecture, University of Edinburgh, School of Law. Edinburgh, 7.7.2011. AHRC/SCRIPT and BILETA Policy Forum, 7-8.7.2011, University of Edinburgh, John McIntyre Conference Centre. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2011/11-07-07_Speech_Edinburgh_EN.pdf

Heinonen, Risto (2008), There is no privacy in the everyday information society. In: Paratiisi vai panoptikon? - näkökulmia ubiikkiyhteiskuntaan. Päivikki Karhula (toim.). 2008. 192 s. http://lib.eduskunta.fi/dman/Document.phx?documentId=zs00710133927861&cmd=download

Howe, Daniel C. & Nissenbaum, Helen (2008), Track me not: resisting surveillance. In: Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society.

Kerr, Ian & Steeves, Valerie & Lucock, Carole (ed.). Oxford: Oxford University Press (2008).

IFLA (2011), IFLA Statement on Intermediary Liability for the IGF. Internet Governance Forum (IGF), Nairobi, Kenya http://www.ifla.org/en/publications/ifla-and-eblida-statement-on-acta-and-the-importance-of-multilateral-multi-stakeholder-

IFLA & EBLIDA (2012), IFLA and EBLIDA Statement on ACTA and the Importance of Multilateral Multi-stakeholder IP Policy Formation. The Hague, 2 July 2012.

IMMI Status Report (2012). April 2012. http://immi.is/images/8/8c/2012-04-15_IMMI_status_report.pdf

Johnston, Ian (2009), EU funding 'Orwellian' artificial intelligence plan to monitor public for "abnormal behaviour". The Telegraph, 19.9.2009. http://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html

Karhula, Päivikki (2012a), Data driven futures. FAIFE Spotlight, 5.6.2012.http://www.ifla.org/faife/spotlight

Karhula, Päivikki (2012b), Information and communication related control in a ubiquitous environment. (Unpublished article)

Kelly, Sanja & Cook, Sarah (2011), New technologies, innovative repression: Growing Threats to Internet Freedom. In: Freedom on the Net 2011: A Global Assessment of Internet and Digital Media. Freedom House. http://www.freedomhouse.org/sites/default/files/inline_images/Overview%20essay%20FINAL%204%2014%202011.pdf

Khaki, Ateqah (2012), Indefinite Detention is Un-American. ACLU Blog of rights. 6.6.2012. http://www.aclu.org/blog/national-security/indefinite-detention-un-american

La Rue, Frank (2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations. Human Rights Council. 16 May 2011. Seventeenth session, Agenda item 3. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Lessig, Lawrence (2011), The Architecture of Access to Scientific Knowledge. Lecture at CERN, Geneva, Switzerland, 18 April 2011. http://vimeo.com/22633948#

Lyon, David (2002), Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination. London : Routledge, 2002.

McDermott, Abigail J. (2012), Copyright: Regulation Out of Line with Our Digital Reality? Information Technology & Libraries. March, 2012, Vol. 31 Issue 1, p7-20. 14p.

Manjikian McEvoy, Mary (2010), From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. International Studies Quarterly (2010) 54, 381–401. https://www.e-education.psu.edu/drupal6/files/sgam/virtual_space/globalvillagevirtualbattlespace.pdf

Monahan, Torin (2010), Surveillance in the Time of Insecurity. Rutgers university press, New Brunswick, New Jersey, and London.

Morozov, Evgeny (2011), The net delusion: the dark side of Internet freedom. New York, NY : PublicAffairs, 2011. The Office of the Data Protection Ombudsman. Data protection in Finland http://www.tietosuoja.fi/28997.htm

Mueller, Milton (2010). Security Governance on the Internet. In: Networks and states: The Global Politics of Internet Governance, 280. MIT Press.

O'Brien, Mark (2010), Law, privacy and information technology: a sleepwalk through the surveillance society? Information & Communications Technology Law. Vol. 17, No. 1, March 2008.

Ohm, Paul (2009), The Rise and Fall of Invasive ISP Surveillance. University of Illinois Law Review, 2009 (5): 1417. http://ssrn.com/abstract=1261344

Osterhaus, Anja & Fagan, Craig (2009), Alternative to silence: Whistleblower protection in 10 European countries. Transparency international, 2009. http://www.transparency.org/whatwedo/pub/alternative_to_silence_whistleblower_protection_in_10_european_countries

REFERENCES

Panitch, Judith M. & Machalak, Sarah (2005), The serials crisis. A White Paper for the UNC-Chalep Hill Scholarly Communications Convocation. Janury, 2005. http://www.unc.edu/scholcomdig/whitepapers/panitch-michalak.html

Pike, George H. (2011), What the Future Holds for Net Neutrality. Information Today, June 2010, Vol. 27 Issue 6.

Presdee, Mike (2000), Cultural Criminology and the Carnival of Crime. London; New York: Routledge, 2000.

Privacy International (2004), Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection. Privacy International in co-operation with European Digital Rights Initiative, the Foundation for Information Policy Research, and Statewatch. February, 2004. http://www.policylaundering.org/issues/travel/transferringprivacy.pdf

Privacy International (2007), The 2007 International Privacy Ranking. Leading surveillance societies in the EU and the World 2007. 28.12.2007.

Privacy International. https://www.privacyinternational.org/reports/surveillance-monitor-2007-international-country-rankings/i-summary-of-key-findings

Privacy International (2011a), Our response to the EU consultation on legality of exporting surveillance and censorship technology. 31.10.2011. https://www.privacyinternational.org/reports/our-response-to-the-eu-consultation-on-legality-of-exporting-surveillance-and-censorship

Privacy International (2011b), Surveillance Monitor 2011: Assessment of surveillance across Europe. 26.1.2011. https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/ephr.pdf

Reporters Without Borders (2011), Internet Enemies. 12 March 2011. http://12mars.rsf.org/i/Internet_Enemies.pdf

Reporters Without Borders (2012), Beset by online surveillance and content filtering, netizens fight on. 13.3.2012. http://en.rsf.org/beset-by-online-surveillance-and-13-03-2012,42061.html

Salminen, Juho (2011), Suomessa miljoona henkilörekisteriä. Isoilta ruumiilta vältytty. Suomen kuvalehti, 9.11.2011. http://suomenkuvalehti.fi/jutut/kotimaa/suomessa-miljoona-henkilorekisteria-isoilta-ruumiilta-valtytty

Saas, Claire (2012), Exceptional Law in Europe with Emphasis on "Enemies". Draft. Conference presentation in: Preventive Detention and Criminal Justice, Ravenna, May 11 – 12, 2012. http://www.law.unc.edu/documents/faculty/adversaryconference/exceptionallawsineuropewithemphasisonenemiesapril2012.pdf

Turow, Joseph (2011), The Daily You. Yale University Press, 2011.

Waugh, Rob (2012). New surveillance cameras will use computer eyes to find 'pre crimes' by detecting suspicious behaviour and calling for guards. Daily Mail Online. Published, 5.6.2012 13:12 GMT, Updated 5.6.2012 13:12 GMT. http://www.dailymail.co.uk/sciencetech/article-2154861/U-S-surveillance-cameras-use-eyes-pre-crimes-detecting-suspicious-behaviour-alerting-guards.html

White, Sonya & Creaser, Claire (2007), Trends in Scholarly Journal Prices. March 2007. Loughborough, LISU, 2007. http://www.lboro.ac.uk/departments/dis/lisu/downloads/op37.pdf

Whittaker, Zack (2012), DoJ sues Apple, publishers in e-book price fixing antitrust suit. ZDNet, 11.4.2012. http://www.zdnet.com/blog/btl/doj-sues-apple-publishers-in-e-book-price-fixing-antitrust-suit/73845

Wu, Tim (2007), Network Neutrality FAQ. Last modified: 25.8.2007. http://www.timwu.org/network_neutrality.html

Hankkeen verkkosivut

http://www.uta.fi/~tl93458/index.html (päivittyy)

Hankkeen julkaisut englanniksi sivuilla http://www.ifla.org/faife/spotlight

FAIFE verkkosivut

Committee on Freedom of Access to Information and Freedom of Expression http://www.ifla.org/faife