Paratiisi vai panoptikon?

Päivikki Karhula (toim.)

Paratiisi vai panoptikon?

Näkökulmia ubiikkiyhteiskuntaan

Päivikki Karhula
(toim.)

EDUSKUNNAN KIRJASTON TUTKIMUKSIA JA SELVITYKSIÄ 10

EDUSKUNNAN KIRJASTO
HELSINKI 2008

© Eduskunnan kirjasto

ISBN 978-951-53-3054-0 (nid)
ISBN 978-951-53-3055-0 (PDF)

PAINOPAIKKA | TRYCKORT
Edita Prima Oy

KANSI | OMSLAG
Graafinen suunnittelu: Heikki Rajala
Kannen kuva: Karen J. Hatzigeorgiou

Sisällys

Johdanto 7

Sähköpaimen - kansalainen ubiikkiyhteiskunnan varjossa
Päivikki Karhula 11

Ubiikkiyhteiskunnan teknologiat 14

Ubiteknologian kääntöpuolet ja vaikutukset 30

Ubiikkiyhteiskunnan ongelmat 48

Läpinäkyvä kansalainen 63

Paratiisi vai panoptikon? 67

Lähteet 70

Koodi on lakia vahvempi
Jyrki Kasvi 83

Massojen piilokulttuuria verkossa 83

Välinpitämättömyydestä mediapaniikkiin 84

Teknologia käy lainsäädännön edellä 86

Lainulkopuoliset käytännöt 87

Miten voi ymmärtää tekijänoikeuslainsäädäntöä? 89

Yhteisöllinen ja henkilökohtainen media haastaa käsitteet 91

Paikkatiedon epäselvät pelisäännöt 91

Puuttuva keskustelu kansalaisoikeuksista 93

Kansalaisoikeuksien sirpaleiset periaatteet 94

Kuka valvoo valvojia? 95

Turvallisuuden paradoksit 96

Kansalaisjärjestöt ja ubiikkiyhteiskunta - kuuleeko kukaan
Ville Oksanen 98

Villi ja vapaa Internet 98

EFFI verkkokäyttäjien edunvalvojaksi 100

EFFI ja tekijänoikeuslain uudistaminen 101

EFFI ja ohjelmistopatentit 105

EFFI ja Enforcement-direktiivit 108

Sähköinen sananvapaus ja teletietojen tallennusvelvollisuus 111

Poliittisen toiminnan mallit 112

Kansalaisjärjestön mahdollisuudet 114

Kansalaisvaikuttaminen ja ubiikkiyhteiskunta 115

Oikeudellinen tieto verkkoyhteiskunnassa
Ahti Saarenpää 117

Oikeudellinen tieto ja tietotekninen kehitys 117

Oikeaa tietoa oikeaan aikaan 117

Lakien määrä lisääntyy ja lait monimutkaistuvat 118

Lainsäädäntö on prosessin tulos 119

Kohden parempaa lainsäädäntöä 119

Lakien sisältö pirstaloituu 120

Oikeudelliset tietovarannot 121

Maksuttomat oikeudelliset perustietovarannot 122

Oikeudellisen tiedonhaun ongelmat 122

Oikeudellinen tieto on sosiaalista pääomaa 123

Miten oikeudellinen tieto löytää lukijan? 123

Oikeus ja sen tulkinta verkoissa 130

Kansalainen lakitekstien lukijana 130

Lakitekstien käsitteet ja oikeuslähdeoppi 131
Kansainvälistymisen vaikutukset 132
Web 2.0 ja yhteisöllinen tiedontuotanto 134
Parviälyä vai omatekoista asiantuntijuutta? 134
Tieto etääntyy käyttäjästä 136
Laadukas tieto, hakutaidot ja laintulkinta avaimina demokratiaan 137

Kansalaisen oikeudet tiedon valtatiellä
Ahti Saarenpää 141
Tietoyhteiskunnasta verkkoyhteiskuntaan 141
Uuden infrastruktuurin vaikutukset 142
Lainsäädäntö ja infrastruktuuri 144
Demokraattinen oikeusvaltio ja kansalaisen perusoikeudet 145
Oikeusvaltio ja verkkoyhteiskunta 146
Tietotekniikka ja oikeudellinen tutkimus 147
Oikeusinformatiikka 148
Infrastruktuuri sääntelyn kohteena 149
Verkkojen muutos haasteena 150
Tiedon valtatie kaipaa liikennesääntöjä 152
Internet-oikeus vai informaatio-oikeus? 154
Informaatio-oikeuden periaatteita 155
Lainsäädännön ja verkon haasteet käyttäjälle 158
Arjen tietoyhteiskunnan jännitteet 159
Lopuksi 161

Arjen tietoyhteiskunnassa ei ole yksityisyyttä
Risto Heinonen 162

Ubiikkiympäristön tiedonkeruu 162

Valvontayhteiskunnan kehittyminen 171

Onko ubimaailmassa yksityisyyttä? 180

Lainsäädäntö ja yksityisyys 185

Kirjallisuutta 189

Johdanto

Ubiikki- eli kaikkialle ulottuva tietoteknologia (ubicom, ubiquitous computing) on tekemässä tuloaan yhteiskuntaan. Ubiikkiyhteiskunta kuvaa uudenlaista tietoteknologista ympäristöä, jossa tietojenkäsittely sulautuu arkiseen ympäristöön – digitaalisiin- ja mobiililaitteisiin, sirukortteihin, tilojen rakenteisiin, esineisiin ja kehoon. Kun ubiteknologia yleistyy, sen tuntosarvet arkisessa ympäristössä tulevat kirjaimellisesti ”kaikkialla läsnäoleviksi”.

Ubiikki näkyy käyttäjille erilaisina läsnä- ja täsmäpalveluina. Niiden raaka-aineena on erityisesti tapahtumatieto, jonka digitaaliset laitteet, sovellukset ja tietojärjestelmät keräävät ja yhdistelevät entistä älykkäämmin eri puolilta verkon kautta käyttöön. Tunnistuksen ja paikannuksen menetelmät tekevät tietojenkäsittelystä entistä tarkempaa ja henkilökohtaista. Ubiikin uudet mukavuudet tarjoavat helppoutta.

Ubiikkiyhteiskuntaa on kutsuttu myös ”arjen tietoyhteiskunnaksi”. Kaikkialle leviävä tietoteknologia koskettaakin jokaista kansalaista. Se välittää tietoa arkeen, mutta myös kerää tietoa arjesta erilaisiin käyttötarkoituksiin. Ubimaailman vaikutukset voivat siis olla kaksisuuntaisia, mutta myös käänteisiä. Panoptikon, jokaisen arkeen kaikkialla ulottuva ja sitä tarkkaileva ympäristö, voisi olla sen äärimmäinen muoto.

Ubiikkiteknologian tiedonkeruu ja tietojen käyttö tulee muuttamaan arjen rajoja ja niihin liittyviä oikeudellisia käsityksiä. Muutospaineet kohdistuvat erityisesti kansalaisen yksityisyyteen ja tietosuojaan, mutta ne ravistelevat myös laajemmin lainsäädäntöä, oikeudellisia käsitteitä ja yhteiskunnan toimintaperiaatteita. Ubiteknologian paikantamisen, tunnistamisen, tiedonkeruun ja sen hyödyntämisen käytännöt etsivät tämän kehityksen myötä uomiaan.

Julkinen keskustelu suomalaisesta ubiikkiyhteiskunnasta on vasta alussa. Teemaa ovat käsitelleet lähinnä teknologian kehittäjät. Ubiikkiympäristön vaikutukset kulkeutuvat kuitenkin jokaiselle kotiovelle. Olisikin tarpeellista tuoda sen näköaloja ja ongelmia laajempaan keskusteluun.

Taustalla on myös huoli siitä, millainen maailma lopulta tulee ulottumaan jokaisen arkeen. Miten ubiikkimaailman oikeudet ja pelisäännöt muodostuvat? Se, millaiset puolet teknologisen kehityksen myötä tulevat hallitseviksi, on kysymys, johon vastataan osin ubiikkiyhteiskuntaa rakennettaessa. Siksi näiden kysymysten aika on juuri nyt.

Tähän julkaisuun on koottu puheenvuoroja ubiikkiyhteiskunnasta ja digitaaliseen tietoon liittyvistä oikeudellisista kysymyksistä. Kirjoittajat käsittelevät teemoja informaatio-oikeuden, politiikan, tiedonhallinnan, tietosuojan ja kansalaistoiminnan näkökulmista.

AHTI SAARENPÄÄ kuvaa kansalaisen tiedollisia ja perusoikeuksia ja niiden kehityskulkua suomalaisessa tietoyhteiskunnassa. Saarenpää tuo esille monin esimerkein tietoteknologisen kehityksen oikeudellisia haasteita ja niiden ratkaisuiksi kehittyneitä periaatteita. Saarenpää toimii yksityisoikeuden professorina Lapin yliopistossa ja on informaatio-oikeuden tunnetuimpia asiantuntijoita.

VILLE OKSANEN esittelee kansalaisten sähköisiä oikeuksia puolustavan kansalaisjärjestö EFFI:n toimintaa ja historiaa. EFFI on kansalaisten edunvalvojana tuottanut lukuisia kannanottoja ja lainsäädäntötyöhön liittyviä asiantuntijalausuntoja. Järjestössä seurataan tiiviisti tietoteknologiaan liittyvää suomalaista ja EU-lainsäädäntötyötä. EFFI:n kiinnostuksen kohteena ovat olleet myös sananvapauteen ja tiedonkeruuseen liittyvät kysymykset, jotka tulevat vastaan ubiikkiympäristön rakentamisessa. Oksanen on juridiikkaan, politiikkaan ja informaatioteknologiaan perehtynyt oikeustieteen kandidaatti, EFFI:n perustajajäsen (2002) ja nykyinen varapuheenjohtaja.

JYRKI KASVI kuvaa tietoteknologisten teemojen käsittelyä lainsäädäntötyössä ja poliittisessa päätöksenteossa. Kasvi nostaa esille myös esimerkkejä ubiikkiteknologiaan liittyvistä avoimista kysymyksistä. Kasvi on tekniikan tohtori, vihreiden kansanedustaja ja eduskunnan tulevaisuusvaliokunnan jäsen (2003 -). Hän on tunnettu aktiivisesta toiminnastaan tietoteknologiaan ja politiikkaan liittyvissä kysymyksissä sekä lukuisista tietoteknologiaan liittyvistä kirjoituksistaan, joita hän kommentoi myös laajaa suosiota saaneessa blogissaan.

RISTO HEINONEN käsittelee kirjoituksessaan kansalaisen kapenevan tietosuojan ja yksityisyyden uhkaa, joka näyttää etenevän ubiikkiyhteiskuntaa kohden kuljettaessa. Heinonen toimii ylitarkastajana tietosuojavaltuutetun toimistossa. Hän on kirjoittanut lukuisia tietosuojaan liittyviä artikkeleita ja lehtikirjoituksia. Heinonen on pohtinut myös kirjassaan, ”Digitaalinen minä” (2001), digitaalista identiteettiä osin ubiikinomaisia käyttöjä ennakoiden.

PÄIVIKKI KARHULA kokoaa kuvaa ubiikkiympäristön teknologioista ja tiedonhallinnasta. Karhulan tarkastelussa ovat myös ubiikkiyhteiskunnan kääntöpuolet ja kansalaisten vaikutusmahdollisuudet. Karhula toimii verkkotiedon johtavana tietoasiantuntijana Eduskunnan kirjastossa.

Eduskunnan kirjaston tehtävänä on välittää tietoa yhteiskunnasta, oikeudesta ja eduskunnasta. Toivomme tämän julkaisun syventävän ymmärrystä, herättävän keskustelua ja virittävän kiinnostusta ubiikkiyhteiskunnan teemoihin.

Helsingissä, 28.2.2008

Päivikki Karhula

Sähköpaimen – kansalainen ubiikkiyhteiskunnan varjossa

Päivikki Karhula

Ubiikkiyhteiskunta merkitsee kaikkialla läsnä olevaa teknologiaa. Adam Greenfield, puhuu ubiteknologiasta käsitteellä everyware, joka kuvaa hyvin sen tunkeutumista jokapäiväiseen elämään (Greenfield, 2006). Suomenkielessä käytetään useampia termejä, kuten jokapaikan tietotekniikka, sulautettu tietotekniikka, läsnä-äly ja täsmä-äly. Vaikka termit viittaavat hieman erilaisiin puoliin ubiteknologiassa, niiden kohde on pääpiirteittäin sama – langattomassa verkossa toimivat hajautetut järjestelmät, jotka hyödyntävät älykkäämmillä teknologioilla ja sovelluksilla koottavaa tietoa arkisesta ympäristöstä.

> ”Läsnä-äly tarkoittaa tietotekniikan tunkeutumista koko ihmiselämän alueelle: koteihin, matkoille, yksityistilaisuuksiin, julkisille paikoille, töihin, lapsille, aikuisille, julkiseen ja yksityiseen toimintaan.” *(Liikenneministeriö,2006)*

Ubiikkiteknologiat perustuvat hajautettujen tietojärjestelmien, langattomien verkkojen, muistien ja tiedonhallinnan menetelmien kehittyneisiin versioihin ja niiden yhdistelmiin. Toiminnoissa hyödynnetään yhä enemmän tunnistuksen ja paikannuksen menetelmiä.

Ubimaailman tietovarastot ovat massiivisia tai hajallaan olevia yhteiskäyttöisiä tietojärjestelmiä. Niihin voidaan koota tietoa erilaisista tiedonkeruun ympäristöistä ja yhdistellä niiden tietoja erilaisiin tarkoituksiin. Ubimaailma syntyy, kun nämä teknologiat ja tietovarastot kutoutuvat yhteen ja liittyvät verkkoon.

Älykäs tietoteknologia sulautuu esineisiin ja arkiseen ympäristöön. Se kätkeytyy arkipäivän esineisiin, pintoihin ja arkkitehtuuriin älykkäinä ja havainnoivina laitteina (sensorit, anturit). Laitteet ja verkkoyhteydet keräävät ja käsittelevät tietoa jatkuvasti. Ubiteknologian tiedonkeruu on ”aina päällä”.

Ubiikin tietoympäristön raaka-ainetta ovat erityisesti tilanne- ja tapahtumakohtainen tieto, jota kerätään esimerkiksi palveluissa asioinnin tai ympäristössä liikkumisen yhteydessä. Näitä kaupan kassalta, verkkopalveluista, kulkuvälineistä ja tiloista koottuja tietoja voidaan liittää yhteen muuhun kohteesta kerättyyn tietoon, kuten kohteen tai henkilön tausta-

tietoihin, kuviin, ääneen tai havaintodataan.

Käyttäjille ubiikkiympäristön toiminnot näkyvät läsnä- ja täsmäpalveluina, jotka voivat ohjata, suositella tai rajata vaihtoehtoja erilaisissa tilanteissa. Niiden avulla voidaan myös seurata haluttuja asiaintiloja ja saada ilmoituksia uusista tiedoista, poikkeamista tai rajojen ylityksistä. Viranomaisen kiinnostuksen kohteena voisivat olla esimerkiksi kansalaisen eri lähteistä saamat tulot ja julkiset tuet, yrityksiä voisi kiinnostaa kuluttajan luottorajan tarkkailu ja yksityishenkilöä perheenjäsenten sijainnin seuranta.

Havainnoivat ja ympäristöön sulautuvat laitteet

”Why not make the floor ”smart”, and use it to identify and track people?”

- Georgia Institute of Technology, Smart Floor -project

Ubiikkiteknologian käyttöliittymät lakkaavat muistuttamasta tietokonetta. Käyttöliittymät muistuttavat pikemminkin fyysisiä merkkejä havainnoivia tai lukulaitteita. Niistä ei välttämättä löydy näppäimistöjä, eikä näyttöjä.

Ubiikkilaitteet ovat miniskaalan teknologiaa. Niiden muistien, prosessorien ja sensoreiden koko on tyypillisesti korkeintaan senttimetrin suuruinen. Ne voivat olla sisäänrakennettuina esineisiin, joista ei voisi päätellä, että ne sisältävät tietotekniikkaa.

Toimintojen aktivoinnin ja havaintojen tekemisen tapa muuttuu ubiikkiympäristössä. Toiminnot voivat aktivoitua lukulaitteiden, sensorien tai anturien tunnistamien havaintojen ja signaalien perusteella. Laitteet ja sovellukset voivat toimia itsenäisesti ja viestiä keskenään ilman käyttäjän tietoista puuttumista niiden toimintaan.

Ubiikkilaitteet ovat aina päällä tai valmiustilassa vastaanottamaan signaalit kohteesta. Kohde tai sen tila tunnistetaan fyysisten merkkien, kuten kuvan, liikkeen, eleiden, äänen tai tilan muutoksen (esim. lämpötila) perusteella. Laitteet voivat välittää tietoa tietokantoihin tai sovelluksille, jotka voivat käynnistää asiaankuuluvia toimintoja havaintojen pohjalta. Esimerkiksi tietyn tilan läpi kävely voisi saada aikaan signaalin, jonka pohjalta henkilölle lähetetään tarjouskuponki tekstiviestinä – tai hälyttää paikalle vartijan.

Tarkimmin ubiikkiympäristön tiedonkeruuta kuvaa käsite ”ambient information”, jolla viitataan liikkeellä, keholla ja eleillä nopeasti, intuitiivisesti ja huomaamattomasti tuotettavaan tietoon. Käyttäjä ei enää ole

samalla tapaa tietoisesti syventynyt ja keskittynyt laitteiden käyttöön. Tiedonkeruu sulautuu arkielämän toimiin, jossa tiedonkeruu ei edellytä käyttäjältä keskittynyttä tietoisuuden tasoa.

> ”Ambient displays normally communicate on the periphery of human perception, requiring minimal attention and cognitive load. Perceptual bandwidth is minimized; users get the gist of the state of the data source through a quick glance, aural refocus, or gestalt background ambience.” *(Ambient Displays Research Group)*

Nopeus, intuitiivisuus ja helppous

Ubiikkiteknologian avulla syntyy nopeasti ja laajasti tietoa keräävä, analysoiva ja näiden tietojen perusteella automaattisesti toimintoja käynnistävä tietoympäristö. Sensorien, lukulaitteiden, valvontakameroiden ja verkkopalvelujen keräämää tietoa voidaan myös yhdistellä ja rakentaa niistä uudenlaisia palveluja. Tehokkaammat tiedonkeruun, yhdistelyn, analysoinnin ja reagoinnin välineiden yhdistelmänä luovat kokonaan uudenlaisen tietoympäristön.

> ”Everyware recombines practices and technologies in ways that are greater than the sum of their parts.”
>
> *(Greenfield, 2006)*

Nopeat ja huomiota herättämättömät tiedonkeruun ja analysoinnin välineet, joiden tietoja voidaan myös ajantasaisesti analysoida yksilö- tai ryhmätasolla, ovat herättäneet ihastusta jo teknologian varhaisten soveltajien mielessä.

> ”The idea of having true real-time, dynamic, immediate access to supply chain information (and any other type of application information, for that matter), without labor, with the corresponding idea that everything and anything can be serially and individually tracked and recorded (depending on the context) in the RFID chip or over the Internet without the knowledge of the consumer, boggles the mind of most people.” *(Duris, 2003)*

Samoin on tunnistettu mahdollisuudet pidemmälle menevään automatisointiin, jossa ”älykkäät kohteet viestivät toisilleen”. Nämä toiminnot ovat monelta osin jo olemassa.

> ”It gets even more interesting. What happens when individual serialized items are intelligent enough to interact with other ”intelligent” items? Think it’s coming? Think again--it’s already here.”
>
> *(Duris, 2003)*

Uuden tietoympäristön vetovoima, samoin kuin sen ongelmat, ovat sen nopeudessa, ennakoimattomuudessa, intuitiivisuudessa ja tehokkuudessa. Käyttäjästä kertyy palvelun tuottajalle jatkuvasti valtava määrä havaintoja, jotka voidaan analysoida ja niihin voidaan reagoida nopeasti. Ubiteknologian käytön ja väärinkäytön mahdollisuudet ovat moninaiset, niiden vaikutukset kohteiden liikkeisiin ja käyttäytymiseen tuntuvat – ja ne tapahtuvat nopeasti.

Ubiikkiyhteiskunnan teknologiat

”The future exists today. It is just unevenly distributed.”
- William Gibson

Matka ubiikkiyhteiskuntaan on asteittainen, kerroksinen ja ehkä kuoppainenkin. Ubiikkiteknologian kehittämissuunnitelmissa viitataan usein vuoteen 2015. TEKES:in suunnitelmissa puhutaan 5-10 vuoden sisällä odotettavasta kehityksestä (Tekes & Suomen akatemia, 2006b). Japanissa ja Etelä-Koreassa on jo otettu etumatkaa, samoin kuin USA:ssa, jossa erityisesti valvonnan ja tiedonhallinnan teknologiat ovat kehittyneet 2000-luvulla.

Ubiikkiyhteiskunta edellyttää uudenlaista infrastruktuuria, johon kuuluvat yhteensopivat teknologiat ja palvelut sekä niihin liittyvät standardit ja lainsäädäntö. Koska siirtymässä on kyse teknologisesta murrosvaiheesta, siihen liittyviä ratkaisuja ja suunnitelmia ei tehdä vain poliittisten toimijoiden taholla, vaan myös teknologiayrityksien ja standardisoimisorganisaatioiden neuvottelupöydissä. Lainsäädännöllä voidaan kuitenkin ohjata ja säädellä ubiteknologian käyttöä, väärinkäyttöä ja sen vaikutuksia suhteessa kansalaisten elämään.

Ubiikkiympäristö ei ole vain tulevaisuutta, vaan monet osat siitä ovat jo toiminnassa tai rakentumassa askel askeleelta. Kokonaiskuvasta puuttuvat vielä vain teknologioiden kypsyminen, infrastruktuurin laajentuminen, oikeudelliset ratkaisut ja lopulta eri osien liittäminen yhteen. Ubiikkiyhteiskunnan pelisäännöt rakentuvat tämän kehityksen myötä.

Teknologioiden tietyt osat ovat pidemmälle kehittyneempiä kuin toiset ja ne kehittyvät eri tahdissa. Ubimaailman infrastruktuuri edellyttää laajemman käyttöönoton kannalta riittävää kapasiteettia muisteilta sekä laajakaistaista ja automaattisesti yhteyksiä tunnistavaa ja siirtävää verkkoa. Suomessa verkot eivät vielä täydessä laajuudessaan puhu ubimaailman kieltä. Ubiteknologian kehittäjät vaativatkin valokuituverkon laajentamista tai radiotaajuuksiin perustuvan verkon käyttöönottoa,

jotta monimuotoisen median edellyttämät gigabittien nopeudella toimivat tietoliikenneyhteydet tulisivat mahdollisiksi (Liikenneministeriö, 2006).

Ubimaailmassa erilaiset tiedonkeruuympäristöt, tietojärjestelmät ja tietovarastot pyritään saamaan yhteiskäyttöisiksi. Verkottuminen ja digitaalinen konvergenssi eli laitteiden yhdentymiskehitys on luonut perustan tietojärjestelmien yhteentoimivuudelle. Tietokoneiden ja muiden digitaalisten laitteiden, kuten television, musiikkilaitteiden, videoiden, pelien, kameroiden, puhelimien, kaukosäätimien, hälyttimien, anturien ja sensorien toiminnallisuutta voidaan yhä enemmän yhdistellä. Samalla laitteet ja ohjelmat sulautuvat toisiinsa ja fyysiseen ympäristöön ja tulevat helppokäyttöisemmiksi. Kun laitteet kytkeytyvät verkkoon ja niiden toiminnallisuuksia ja tiedonkeruuta voidaan yhdistellä, syntyy ubimedia. *(Karhula, 2003)*

Tietojärjestelmien yhteiskäyttöisyyttä tukevat standardit ja ns. avoimet rajapinnat, joiden tuella yhteyksiä erilaisten tietojärjestelmien välille voidaan luoda yksinkertaisemmin tai liittää niihin lisäpalveluja. Sisältöjen yhteensopivuutta ja tietojen vaihtoa edistävät tietorakenteita ja tietojen haettavuutta yhtenäistävät standardit ja formaatit, kuten XML ja RDF.

Tuloaan tekevät myös yhä tehokkaammat ja älykkäämmät välineet tietosisältöjen analysointiin ja paikantamiseen sekä tietojärjestelmien suunnitteluun ja etähallintaan. Lisääntyvällä älykkyydellä voi olla käänteentekevät vaikutukset, vaikka se toimisi karkealla tasolla, jos sen toiminnallisuus liitetään yleiskäyttöisiin sovelluksiin, kuten hakupalveluihin tai selaimiin. Ubiikkiympäristön keskeisten sovelluksien joukossa mainitaan mm. käyttöympäristöön sopeutuvat ja käyttäjän toiminnasta oppivat ja sitä ennakoivat sovellukset, tiedonkeruun järjestelmät sekä paikantamista ja tunnistamista tukevat sovellukset (TEKES, 2002). Näiden tuella rakentuu ubiikin tiedonhallinta.

(Karhula, 2001, Karhula 2003)

Tunnistus, paikannus ja yksilöinti ovat ubiikkimaailman kulmakiviä. Kun verkosta ja fyysisestä ympäristöstä kootut sähköiset tiedot ja havainnot voidaan yhdistää tiettyyn yksilöön, halutut toimenpiteet voidaan samoin kohdistaa tarkasti henkilö- tai esinetasolle. Läsnä- ja täsmäpalvelut edellyttävät käyttäjän tunnistusta tai paikannusta. Siksi juuri RFID-tunnistus, GPS-paikannus ja niiden kytkennät reitittäviin langattomiin verkkoihin (mesh networking), ovat ubiikin keskeisiä teknologioita (Greenfield, 2006).

Ubiikkimaailman edellytyksiin kuuluu myös all-ip-ympäristö. Ip-

osoitteiden avulla tunnistetaan eri puolella maailmaa sijaitsevat laitteet yksilöivän tunnuksen avulla. Sen avulla voidaan tehdä päätelmiä paitsi tiedon alkuperästä, myös sen reiteistä verkkoliikenteessä. Kun ip-osoitteiden käyttö laajentuu arkiympäristön esineisiin, pintoihin, tiloihin ja henkilöihin, ne merkitään verkkoliikenteen tunnistamalla tavalla. Samalla syntyy yhä syvempi kosketuspinta arjen ympäristöön, joka edistää sen saamista verkon kautta hallittavaksi. *(Greenfield, 2006)*

All-ip-ympäristö, jossa mikä tahansa kohde voitaisiin merkitä verkossa tunnistettavaksi ja paikannettavaksi, on jo standardin tasolla valmis ubimaailman mittakaavaan. IP-osoiteavaruuksien uudet määritykset Internet Protokollan versiossa IPv6, laajentavat halutuille kohdehenkilöille, esineille tai laitteille sopivan osoiteavaruuksien merkintäsyvyyden maapallon jokaiseen kolkkaan hiekanjyvien tarkkuustasolle. Se antaa kaikkialle ulottuvat välineet tiedonhallintaan ja kontrolliin verkossa millimetripaperin mittakaavalla.

> ”…IPv6, provides for an enormous expansion in the available address space – enough for every grain of sand on the planet to have its own IP address…Why specify such abyssal reaches of addressability, if not to allow every conceivable person, place and artefact to have a comfortable spread of designators to call their own?” *(Greenfield, 2006)*

RFID ja kohteiden tunnistus

> *”We’ll put a radio frequency ID tag on everything that moves in the North American supply chain.”*
>
> *- Steven Van Fleet*

Yksilöivän tunnistamisen ja tilanne- ja tapahtumakohtaisen tiedonkeruun mahdollistaa erityisesti RFID-teknologia, joka perustuu muistia sisältävien sirujen ja niitä lukevien laitteiden hyödyntämiseen. Sitä voidaan käyttää henkilöiden, tilojen, esineiden tai eläinten tunnistamiseen ja paikantamiseen.

RFID (Radio frequency identification) eli langaton radiotaajuuksilla tapahtuva tunnistus, perustuu muistia sisältävän mikrosirun ja radiolähettimen yhdistelmään. Sirut voivat olla passiivisia tai aktiivisia. Edelliset edellyttävät lukemista lukulaitteelta, jälkimmäiset voivat myös lähettää tietoa ja ovat etäluettavissa.

Sirujen käyttö on voimakkaasti leviämässä. Yksinomaan sirukortteja myytiin maailmalla 2,6 miljardia korttia vuonna 2005 (Autio, 2006).

Vuoteen 2010 mennessä sirutuotannon arvioidaan nousevan 33 biljoonaan (Sciannamea, 2006).

Muistisiru voidaan liittää kortteihin, kiinnittää tarroina tai muilla tavoilla esineisiin tai rakenteisiin tai asentaa eläimen tai ihmisen kehoon. RFID-siruja on liitetty maksu- ja luottokortteihin, passeihin, henkilökortteihin ja matka- ja kulkukortteihin. Sirutarroja on käytetty esimerkiksi kulutustavaroissa, kirjastojen julkaisuissa, potilaiden tai vankien rannekkeissa. Karjaa ja lemmikkieläimiä sirutetaan monissa maissa. Sirut kätkeytyvät yhä useammin osaksi arjen välttämättömiä esineitä, kuten auton avaimiin, kännyköihin ja mobiililaitteisiin. Kehon toimintaa tai ympäristön tilaa mittaavat anturit tai sensorit ovat myös tulossa osaksi sovelluksia (Honkanen, 2002).

Siruihin perustuvan tunnistuksen avulla voidaan kerätät kohteeseen ja hänen toimiinsa liityviä tietoja. Niiden perusteella voidaan seurata ja analysoida esimerkiksi tietyn henkilön kulutuskäyttäytymistä ja asiointia. Näkyviä RFID-lukijoita, joihin henkilön tai esineen tunnistetiedot luetaan, löytyy esimerkiksi kaupan kassoilta, liikennevälineistä, sairaaloista ja kirjastoista.

Ubiikkimaailman arkkitehtuuria kuvaillaan toisaalta erityisesti näkymättömien lukijoiden ympäristönä. Henkilöt ja kohteet, jotka kantavat etäluettavaa sirua, voidaan tunnistaa vaatteiden ja arkkitehtuurin rakenteiden läpi, olivatpa ne paikallaan tai liikkeessä. Sirujen etäluentaan voidaan yhdistää myös satelliittipaikannuksen ja langattomien verkkojen teknologioita, joiden yhdistelmillä kohde saadaan paikannettua hyvinkin tarkasti (mm. RTLS-teknologia) (Holloway, 2007).

RFID-teknologian ennakoidaan tuovan syviä, henkilökohtaisia ja kaikkialle ulottuvia vaikutuksia yhteiskuntaan. On jopa väitetty, että sen tuoma käänne on verrattavissa sähkön keksimiseen.

> ”RFID is a big deal. Its impact will be pervasive, personal and profound. It will be the biggest deal since Edison gave us the light bulb.” *(Duris, 2003)*

Vaikutukset eivät johdu RFID:stä sinänsä. Liikevaihdon nousu ei synny siruista, vaan sovelluksista ja laitteista, joissa siruja hyödynnetään (Yrjölä, 2003). Kyse on siitä lisäarvosta, mikä sirujen avulla kerätyistä tiedoista saadaan, kun ne yhdistetään muihin tietoihin ja erilaisten sovelluksien toimintoihin. Sirujen käytöstä saadaan erilaisia rationalisoinnin etuja - toimintoja voidaan automatisoida, palveluja nopeuttaa, prosesseja yhdistellä ja työvoimaa vähentää.

RFID:tä hyödyntävät sovellukset ovat laajentuneet ja monipuolistuneet nopeasti. Sirujen etuna viivakoodeihin nähden pidetään erityisesti

etätunnistusta, joka mahdollistaa tuotteiden, kuljetusten ja kohdehenkilöiden seurannan (Yrjölä, 2003). RFID-tunnistusta ja siihen pohjautuvaa tapahtumatiedon seurantaa on kohdistettu eläimiin, ihmisiin, kulutustavaroihin tai liikkeellä oleviin kuljetuksiin. Kanadassa karjan sirutus on ollut pakollista vuodesta 2001 (Canadian Cattle Identification Agency, 2005). Wal-Mart, maailman laajin vähittäistavarakauppaketju, ilmoitti tavarantoimittajilleen 2004 siirtyvänsä tuotteidensa RFID-tarroitukseen varastojen hallinnan ja tuotevirtojen tehostamiseksi. (Business week, 2004). Suomen posti on kokeillut kuljetuksiensa seurantaa RFID-tarroitettuina ja on suunnittelemassa tulevaisuudessa myös postilähetysten seurantaa (Pienimäki, 2006).

Tunnistuksen ja paikannuksen menetelmiä yhdisteltäessä syntyy erilaisiin tiloihin ja ympäristöihin ulottuva ja haluttaessa kohteen etäältä tunnistava, hänen sijaintinsa paikantava ja kulkureittejään seuraava tietoympäristö. Kun sovelluksiin liitetään visuaalisia käyttöliittymiä ja tilakarttoja, niiden avulla voidaan tarkkailla esimerkiksi RFID-tarroitettujen matkustajien kulkureittejä ja sijaintia lentokentillä (Ström, 2006).

Kun tunnistus- ja paikannus tietoja yhdistellään edelleen muihin taustatietoihin ja toimintoihin, voidaan kehittää erilaisia varastojen, jakeluketjujen ja kuljetusten hallinnan sovelluksia tai turvallisuusjärjestelmiä. Niiden avulla nähdään esimerkiksi, mitä varastoista puuttuu, missä on tilaa tai minne liikenne ruuhkaantuu. Älykkäiden teknologioiden avulla tilanteiden hallintaan voidaan kytkeä edelleen lisätoiminnallisuutta, kuten automaattisia tilauksia loppuunmyydyistä tuotteista, hälytyksiä koulutunneilta poissaolevista oppilaista tai lennolta puuttuvista matkustajista.

Ubiikkiyhteiskunnassa ennakoidaan RFID-teknologian avulla koottujen tunnistetietojen ja niitä hyödyntävien tietojärjestelmien kytkeytyvän edelleen osaksi erilaisia laajempia yhteiskäyttöisiä tietojärjestelmiä ja älykkään teknologian sovelluksia (Knuuttila, 2006). Kokonaisuudessa yhdistyvät yksilön tunnistus ja paikannus, reaaliaikainen tiedonkeruu, massiiviset tietovarastot ja tehokkaat tiedon analysointimahdollisuudet erilaisia tarkoituksia varten.

Identiteettien hallinta

Ubimaailman toteutumisen edellytyksenä pidetään sitä, että ihmisillä olisi jatkuvasti päällä oleva langaton yhteys ja sähköinen identiteetti, jonka avulla käyttäjä tunnistetaan. Se luo perustan käyttäjistä tehtävälle tiedonkeruulle ja heille tarjottavalle täsmätiedon jakelulle.

> ”Ubimaailmalle luonteenomaista on se, että ihmiset ovat käytännössä koko ajan yhden tai useamman langattoman viestintäteknologian tavoitettavissa ja voivat sekä saada että lähettää viestejä ja mediaan niiden kautta. Tämä kuitenkin edellyttää lähes välttämättä sitä, että käyttäjien laitteilla on yksilöivä elektroninen identiteetti, joka tulee langattoman liityntäverkon tietoon. Tätä kautta käyttäjien liikkumista, viestintää ja mediakulutusta voidaan seurata kaikissa arkisten elämän paikoissa ja tilanteissa.”
>
> *(Liikenneministeriö, 2006)*

Sähköisen identiteetin ja langattoman jatkuvasti päällä olevan laitteen yhteisvaikutus on siis kokoaikainen ja täsmällinen seurattavuus. Se mahdollistaa käyttäjien liikkumisen, viestinnän ja asioinnin jatkuvan ja kaikkialle ulottuvan valvonnan. Yksilön tunnistaminen antaa yleisavaimen ubimaailman tiedonhallintaan.

Yksilöinti nopeuttaa myös tiedonhallintaa ja hakua. Verkkotiedonhaku aiheen mukaan on vielä Google-aikanakin pitkälle ratkaisematon yhtälö. Esimerkiksi monikielisyys, eritasoinen aiheen kuvailu, synonyymit ja termien väärinkäyttö ovat edelleen esteinä tiedonhakujen täsmällisille osuvuudelle.

Yksilöivän tiedon haku on moninkertaisesti helpompi tehtävä. Jos tieto sisältää yksiselitteisen, globaalisti yksilöivän ja kieliriippumattoman tiedon, kuten RFID-tunnisteen tai ip-osoitteen, käytössä on nopea yleisavain kaikkeen tiettyyn henkilöön liittyvään tietoon.

All-IP-ympäristö on tärkeänä osatekijänä yksilöivässä ja kommunikoivan kohteen tunnistavassa teknologiassa. Internet-verkon tiedonsiirto perustuu tietoliikenneverkkoihin, joiden tieliikennesäännöt perustuvat internet-protokollaan (IP). Kun lähitulevaisuudessa kaikki merkittävät tietoliikennepalvelut tulevat toimimaan IP-protokollan päällä, edellyttää tunnistaminen ja paikannus myös kytkentöjä verkon yleisiin liikennesääntöihin. (Liikenneministeriö, 2006)

Jokaisella verkko- tai puhelinyhteydellä tulee olla laitteeseen kytkeytyvä IP-osoite. Kun kaikki verkot voivat tunnistaa yhtenäisillä säännöillä merkityt laitteet ja laitteet on merkitty IP-osoittein, on kohteet kaikkialla tunnistava ja niitä hallitseva ympäristö valmis. Ubimaailman tietoliikenteessä IP-osoitteet eli verkon tieliikenteen katuosoitteet yltävät millimetripaperin tarkkuuteen.

IP-osoitteen rajoituksena on, että se on looginen, eikä fyysinen. Siitä ei voi suoraan päätellä sijaintia samaan tapaan, kuin esimerkiksi postinumerosta. Osoitteiden fyysisen sijainnin jäljittämiseksi on kuitenkin

kehitetty apuvälineitä, joilla myös fyysinen sijainti saadaan helposti selville.

Esimerkiksi Geoselect tarjoaa IP-karttoja (IP mapping services), joiden perusteella käyttäjä jäljitetään kartalta IP-osoitteen perusteella. Hostip.info palvelu antaa samankaltaisen välineen kenelle tahansa verkkokäyttäjälle. Yritykset käyttävät IP-osoitteen jäljityspalveluja esimerkiksi erotellakseen asiakkaat, jotka tulevat luotettavuuden kannalta epäilyttäviltä alueilta (”high-risk IP address”) tai kohdistaakseen markkinointia tietyn alueen asiakkaille. *(Lessig, 2006)*

Monissa tietoympäristöissä IP-osoite on dynaaminen eli vaihtelee, jolloin ei saada varmuutta käyttäjästä. Jos laitteita voidaan käyttää ainoastaan lukemalla sille käyttäjän tunnistava siru, kuten sirullinen henkilökortti, jäljitetään aina myös laitteen käyttäjä. Laite tunnistaa silloin jokaisen käyttäjän tai esineen, joka käsitellään sen kautta.

RFID-teknologia ja sirujen käyttö on tullut juuri edellä kuvatuista syistä tarpeelliseksi osaksi ubiikkimaailman rakenteita. Ne kiinnittävät varmuudella tunnistukseen tiettyyn henkilöön, esineeseen, laitteeseen tai tilaan. Esimerkiksi sähköisen asioinnin ns. vahva tunnistus ja sähköinen identiteetti perustuvat myös käyttäjän sirukortin ja lukulaitteen yhdistelmään ja sitä kautta tapahtuvaan yksilöintiin.

Tunnistettujen käyttäjien käyttöoikeuksia tietojärjestelmissä voidaan hallita erilaisin järjestelmin. Keskitetyillä identiteettien hallintajärjestelmillä voidaan säädellä käyttäjän pääsyä joukkoon erilaisia tietojärjestelmiä ja sovelluksia, mutta myös sovelluksien käyttöoikeuksia eli niiden toimintojen tasoa, jotka ovat käyttäjille mahdollisia.

Tunnistuskäytännöt ovat yleistymässä paitsi sähköisen asioinnin, mutta myös erilaisten monitoimikorttien ja tietojärjestelmien yhteiskäytön laajenemisen takia. Tietojärjestelmien yhteiskäyttöä tukeva keskeinen tunnistamis- tai autentikointikäytäntö on kertakirjautuminen eli SSO (single-sign-on), jonka avulla käyttäjä saa pääsyn yhdellä kertaan useampiin palveluihin. Esimerkiksi suomalaisissa yliopistoissa on käytössä kertakirjautuminen ja ns. federoitu identiteetti, joka mahdollistaa kertakirjautumisella korkeakoulujen sisäisten tietojärjestelmien käytön, mutta antaa samalla kertaa käyttöoikeudet myös joihinkin muihin korkeakoulujen ulkopuolisiin tietojärjestelmiin (Linden, 2005, Teräs, 2005, CSC & Suomen yliopistojen ja korkeakoulujen ATK-keskukset, 2004).

Monitoimikortteja käytetään laajalti esimerkiksi suomalaisissa korkeakouluissa ja ns. virkakortti tekee tuloaan julkishallinnon palveluihin. Virkakortin avulla päästään kertakirjautumalla julkishallinnon erilaisten

tietojärjestelmien yhteiskäyttäjäksi. (Kuntaliitto, 2007, Valtionvarainministeriö, 2007a).

Koska identiteetin hallintajärjestelmissä on eroja, eivätkä ne välttämättä keskustele keskenään, on rakenteilla myös niiden välistä liikennettä hallinnoiva ja tulkitseva metatietojärjestelmä. Teknologian vauhdittajana on Microsoft, jonka Identity Metasystem -mallista ollaan kehittämässä ydinsovellusta tai metatietojärjestelmää, jonka avulla erilaisten identiteettijärjestelmien tietoja välitetään toisilleen.

> "The metasystem enables identities provided by one identity system technology to be used within systems based on different technologies, provided an intermediary exists that understands both technologies and is willing and trusted to do the needed translations." *(Rundle & Laurie, 2005)*

Tunnistuskäytäntöjen ja identiteettien hallintajärjestelmien avulla on Internetiin muodostumassa uusi kerrostuma, jossa käyttäjän tietoja ja niiden yhteyksiä sovelluksiin hallitaan. Käyttäjien pääsy eri järjestelmiin voi yksinkertaistua, mutta samalla laajentuu heidän tietojensa, asiointinsa ja verkossa liikkumisensa seuranta. Lisäksi tiedot eri järjestelmistä voidaan koota ja yhdistellä tehokkaammin henkilöihin liittyvien yhtenäisten avaintietojen avulla – tai metajärjestelmän avulla, joka kääntää tiedot eri järjestelmille.

Paikannuksen laajentuminen

Vaihtelevista teknisistä toteutuksista huolimatta, paikannukseen on perustaltaan 3 teknologiaa (Morville, 2006):

- triangulation, jossa yhdistetään useita etäisyyden (lateration) ja kulman (angulation) mittauksia suhteessa kohteeseen
- proximity, jossa mitataan kohteen läheisyyttä suhteessa tiettyyn pisteeseen
- scene analysis, jossa kohde suhteutetaan tiettyyn ympäristöön. Elementteinä voidaan käyttää kuvia, elektromagneettista kohteen tunnistamista tai muita kohteen fyysisiin ominaisuuksiin perustuvia ominaisuuksia

Paikannuksen kielessä puhutaan fyysistä ja symbolisesta paikasta, jossa edellinen viittaa koordinaatein ilmoitettavaan teknisesti tarkkaan sijaintiin (47 39'17'') ja jälkimmäinen sen selväkieliseen muotoon (esim. keittiö). *(Morville, 2006)*

Verkkomaailman avainteknologia paikannukseen on ollut GPS (Global Positioning System), jonka satelliittipohjainen radionavigointi mahdollistaa kohteiden suhteutetun (leveysaste, pituusaste, korkeus ja liikkumisen nopeus) paikantamisen maalla, merellä ja ilmassa. Morvillen mukaan USA:n puolustusministeriön 24 satelliittia paikantavat kohteen tähän teknologiaan perustuen 3 metrin tarkkuudella. Kuluttajille älypuhelimiin, kelloihin, rannekkeisiin, autoon tai muihin laitteisiin kytkettynä tarjolla olevat GPS-paikantimet perustuvat samaan tekniikkaan.

(Morville, 2006)

GPS:n kolmen metrin säde ei kuitenkaan riitä kaikentyyppiseen paikantamiseen sisätiloissa. Täydennyksenä on käytetty muita radiotaajuuksiin perustuvia paikannuksen teknologioita, kuten langatonta verkkoa (WiFi, Bluetooth, Ultra-wideband) ja RFID-teknologiaa. Jos kohde kantaa RFID-sirua, se on tunnistettavissa tuuman tarkkuudella UWB-ympäristössä. *(Morville, 2006)*

Kaikkialle ulottuvan tunnistuksen ja paikannuksen välineet sisältyvät yhä useammin arkisen ympäristön esineisiin ja viestintälaitteisiin, kuten erilaisiin kortteihin, matkapuhelimiin ja kulkuneuvoihin. Kännykkään perustuvan paikannukseen arvioidaan nopeasti lisääntyvän niin, että jo neljän vuoden sisällä 21 miljoonaa ihmistä seurattaisiin paikantavan kännykän välityksellä. Seurantaa hyödyntäisivät esimerkiksi työnantajat ja vanhemmat (Leidenius, 2008). Satelliittipaikannukseen soveltuvien laitteiden autoissa ennakoidaan puolestaan lisääntyvän vuoteen 2010 mennessä siinä määrin, että ne kuuluvat miltei kaikkiin uusiin autoihin (Liikenneministeriö, 2006).

GPS-paikannusta on hyödynnetty monin tavoin myös verkossa. Sen tunnistamat kohteet voidaan liittää erilaisiin visuaalisiin sovelluksiin, kuten karttoihin. Niiden pohjalta on rakenneltu esimerkiksi seikkailupeli ”geocatching”, jossa eri puolelle maailmaa löytyvät kohteet voidaan löytää verkossa ilmoitetun sijainnin mukaan. *(Morville, 2006)*

Sijainnin seuranta ja paikantaminen ovat tulleet jo kuluttajille tarjottaviksi palveluiksi. USA:ssa kuluttajille myydään kenet tahansa paikantavaa palvelua (http://world-tracker.com/).

Sijainnin jäljittämisen lisäksi voidaan seurata liikkumista ja kulkureittejä sekä kytkeä niihin seuranta- ja hälytystoimintoja. Esimerkiksi lasten liikkumisen ja sijainnin seurantaan on tarjolla USA:ssa ”Wherify Wireless GPS Personal Locator for Kids” -palvelu. Seurantaa voi tehdä kartan tai ilmakuvan perusteella ja valvoa lapsen kulkureittejä tai koo-

ta tapahtumahistoriaa lapsen liikkumisesta. Seurannan voi halutessaan ajastaa ja tilata siitä ilmoituksia. *(Morville, 2006)*

Vastaavia paikannuspalveluja on tarjolla nuorten seurantaan. ”Teen Arrive Alive” -palvelu tarjoaa kännykän paikannustietoihin perustuen tietoja nuoren sijainnista, kulkureiteistä ja tapahtumahistoriaa hänen päivittäisestä liikkumisestaan. Vanhemmat voivat lisäksi asentaa nuoren autoon ajonopeutta tarkkailevan sirun (carchip), joka välittää palveluun tiedot nuoren ajotavoista.

Seurantapalveluja on muotoiltu myös aikuisten arkeen, kuten seurustelukumppaneille, pariskunnille, työntekijöille ja työnantajille. Niitä markkinoidaan eräänlaisina lähipiirin luotettavuuden arviointipalveluina. Erilaisille kohderyhmille tarjottavat seurantapalvelut laajentavat käytännössä halutun osapuolen liikkumisen ja sijainnin tarkkailun kenen tahansa maksavan asiakkaan käsiin. *(Andrejevic, 2007)*

Seurantapalveluihin ideoidaan edelleen lisää hienosäätöä ja liitäntöjä muihin teknologioihin. Facebook-yhteisöpalvelussa on käyttäjien henkilötietoihin liitetty Wayfinder-sovellus, jonka avulla käyttäjä voi antaa verkkoystävilleen mahdollisuuden seurata sijaintiaan kartalta (Privat, 2008). HIIT on kehittänyt ns. kontekstipuhelimen, jonka avulla voitaisiin seurata paitsi haluttua kohdehenkilöä, mutta myös hänen lisäkseen muita paikallaolijoita, joilla on puhelin (Liikenneministeriö, 2006). Morville puolestaan toteaa, että sähköinen lapsenvahti voi kertoa lasten sijainnin, mutta ei sitä, mitä paikalla tehdään. Hän arvelee, että lisäarvoa saataisiin, kun seurantaan kytkettäisiin video- ja audiovalvonta. (Morville, 2006)

Paikannuksen ja liikkumisen seurannan sovellukset ovat jo markkinoilla hyötyineen ja haittoineen. Niitä myös yhdistellään esimerkiksi yhteisöllisiin verkkopalveluihin sekä tunnistuksen, tiedonkeruun, tiedon analysoinnin, katselun ja kuuntelun, hälytyksien ja etävalvonnan sovelluksiin. Näiden tarkoitukset voivat olla hyödyllisiä tai haitallisia yhteyksistä riippuen.

Julkinen tiedonkeruu laajentuu ja yhdentyy

> *”We have a capability to gather, store, analyze, segment and use for commercial (and many other) purposes more data about more people than was ever dreamed of.”*
>
> *- Richard Barton, 1995*
> *(O’Harrow, 2005)*

Tiedonkeruuta kansalaisista on tehty vuosikymmeniä, mutta sen luonne on muuttunut vasta 2000-luvulla. Tietovarastot ovat laajentuneet, monipuolistuneet ja tulleet yhteiskäyttöisiksi. Samalla yksilöä tunnistavien tietojen keruu on tarkentumassa ja tunnistuskäytännöt alkavat laajentua erilaisiin asioinnin, liikkumisen ja verkkokäytön tilanteisiin. Kun laajentuviin tietovarastoihin ja tunnistuskäytäntöihin yhdistetään ubiikkiteknologioiden sovelluksia, muodostuu kokonaan uudenlainen tietoympäristö, jossa kansalaisten arkisten toimien seuranta laajentuu merkittävästi.

Kansallisten tietorekistereiden määrä ja niiden sisältämien tietojen ala ovat nopeasti laajentuneet. Teletunnistetietojen tallennusvelvoite laajentaa kännykkä- ja verkkoliikenteen seurannan käytännössä koko väestön kattaviksi rekistereiksi, joita telepalvelujen tarjoajat ylläpitävät (2006/24/EY, HE 158/2007 vp, Sisäasiainministeriö, 2005, Korpimies, 2007). Sosiaali- ja terveystietojen yhdistämiseen ja vaihdettavuuteen on pyritty sähköisen potilastietojärjestelmän ja sosiaalialan tietojärjestelmien rinnakkain edenneissä kehityshankkeissa (Sosiaali- ja terveysministeriö, 2004, Hämäläinen, 2005, Tenhunen 2006). Monitoimikortit ja sähköinen asiointi ovat vauhdittamassa tietovarastojen kokoamista ja yhteiskäyttöä.

Tietojenkäsittelyssä halutaan hyödyntää uudenlaisia tunnistetietoja – biologista ja geneettistä tietoa. Menettelyllä päästään entistä varmempaan käyttäjien tunnistukseen. RFID-pohjainen käyttäjien tunnistus sekä biometristen tietojen yhdistäminen tunnistukseen mahdollistavat myös käyttäjien tunnistuksen erilaisilla kone- ja etäluettavilla menetelmillä.

Tunnistetietoja kootaan yhä laajemmin tietokannoiksi, mikä edistää niiden hyödyntämistä erilaisiin tarkoituksiin. Sormenjälkien tallennus on EU-maissa laajentunut rikollisista turvapaikan hakijoihin (Sisäasiainministeriö, 2003). Sormenjälkien kokoaminen ulottuu kuitenkin koko väestöön 2009, jolloin EU:n passiasetus velvoittaa sormenjälkien käyttöönottoon matkustusasiakirjoissa (U 41/2007 vp.).

DNA-tietokantojen kehittäminen eri maissa on edennyt nopeasti (Privacy International, 2007). Suomessa julkiseen keskusteluun on nostettu viime vuosina koko väestöä kattavan DNA-rekisterin rakentaminen, josta tosin on vastakkaisia käsityksiä (Ora, 2006, STT, 2006a, STT, 2006). Ihmisen kudosnäytteiden ja muiden biologisperäisten näytteiden kokoamista hajautettuun kansalliseen ja kansainväliseen yhteiskäyttöön biopankkeina on myös kiirehditty (Sosiaali- ja terveysministeriö, 2007).

Tunnistuskäytännöt ovat yleistymässä, mutta myös niiden kansainvä-

listä yhdentymistä tavoitellaan. Se näkyy esimerkiksi sähköisen identiteetin kehittämisenä EU-maiden välille (E-Europe Smart Cards Charter, 2003, Porvoon ryhmän -konferenssit, http://www.fineid.fi/vrk/fineid/home.nsf/suomi/porvoo_group).

Ubiikinomainen tietojen hyödyntäminen vaikuttaa olevan seuraava kehityksen askel. USA:ssa kehitteillä on esimerkiksi biometristen tietojen yhdistely paikannuksen, etätunnistuksen ja älykkäiden visuaalisten teknologioiden sovelluksin. Niiden avulla esimerkiksi halutut henkilöt voidaan kasvokuvan perusteella tavoittaa ihmisjoukoista (Nakashima, 2007). Biometrisiä tietoja ei siis käytetä vain tunnistamiseen maan rajoilla, vaan näyttäisi, että niitä tullaan hyödyntämään yhä laajemmin haluttujen henkilöiden jäljittämiseen "kaikkialla". Suunta näkyy myös biometristen tietojen käytön kehittämissuunnitelmissa.

"The long-term goal is "ubiquitous use" of biometrics."
(Nakashima, 2007)

Jo tietovarastojen alan laajentuminen ja niiden yhteiskäyttöisyys laajentavat kansallisen tiedonkeruun skaalaa ennennäkemättömällä tavalla. Kansainväliset sopimukset ja kansainvälisen tiedonvaihdon lisääntyminen ovat kuitenkin edelleen laajentamassa kansallisten rekistereiden käyttöyhteyksiä. Kansallisia tietorekisterejä on sopimuksin voitu avata käytettäväksi rajojen ulkopuolelle tai velvoittaa muuhun tiedon luovutukseen viranomaisten välisessä yhteistyössä. Tällaisia sopimuksia ovat mm. Cybercrime-sopimus ja Prümin sopimus (HE 153/2006, Prümin sopimus, 2007).

Tiedonkeruun laajentumisen, tunnistuksen tarkentumisen, tietovarastojen yhteiskäyttöisyyden ja ubiikkiteknologian sovellusten yhdentymisestä on monia merkkejä. Kehitys näyttäisi etenevän kohden kansainvälistä tietoympäristöä, jossa voitaisiin hyödyntää myös massiivisia kansallisia ja yhteiskäyttöisiä tietovarastoja. Tämän kehityssuunnan vaikutukset voivat olla ennakoimattomia.

Kaupallisen tiedon digitaalinen valtameri

Henkilöihin liittyvä tiedonkeruu on kiihtynyt myös yksityisellä sektorilla 1990-luvulta alkaen älykkäämpien teknologioiden, erityisesti tiedon louhinnan menetelmien myötävaikutuksella. Samalla on saatu vauhtia tietovarastojen laajentamiseen ja tietojen yhdistelyyn. *(O'Harrow, 2005)*

Tiedonkeruun laajimpia toimijoita ovat siihen erikoistuneet yritykset, mutta tiedon jakamiseen osallistuvat monet muutkin toimijat. Yritysten

välinen tietojen vaihto tai yhteiskäyttö näyttää lisääntyvän esimerkiksi strategisissa verkostoissa, joissa tietoja jaetaan. Toimintatavan kantavana ajatuksena on synergiaetujen hyödyntäminen yhteiseen käyttöön jaetusta asiakastiedostosta (“cross selling”). *(Borking, 2005)*

2000-luvun tiedonkeruun laajuutta voisi kuvata digitaalisena valtamerenä, jolle antavat mittasuhteita suurimpien amerikkalaisten tiedonkeruuyrityksien tietomäärät. ChoisePoint, henkilötietoja ja taustaselvityksiä myyvä suurin amerikkalainen yritys, on koonnut tietokantoihinsa yli 17 miljardia tietuetta, jotka koskettavat yli 220 miljoonaa henkilöä. Acxiom, toinen keskeinen amerikkalainen tiedonkeruuyritys, mittaa tietovarastojensa laajuutta petatavuissa (1 PB = 1 048 575 GB). Experian, tiedonkeruuyritys, joka toimii myös Britanniassa, pitää tietokannoissaan tietoja 45 miljoonasta britistä ja 215 miljoonasta amerikkalaisesta kuluttajasta (Lace, 2005).

Kyse ei ole vain henkilön perustiedoista, vaan monista erilaisista kaupallisista ja julkisista lähteistä yhteen kootuista tiedoista. Tietokannat voivat sisältää jopa terveyteen, mielipiteisiin ja kulutuskäyttäytymiseen liittyviä sensitiivisiä tietoja. Nämä tiedot ovat tarjolla maksua vastaan saatavilla laajentuvalle asiakaskunnalle. USA:n tietosuojalainsäädäntö ei estä näitä tiedonkäsittelyn menettelyjä.

> ”Want to have the names, addresses of people taking Prozac for depression? No problem. Computer users who like to gamble online? Who like sex toys? Bible believers and Hispanic political donors? It’s all available to almost anyone who wants to pay”
> *(O’Harrow, 2005)*

Henkilöä koskevan tiedon ala on laaja ja monipuolinen. Tietokannat voivat sisältää mm. sormenjäljet, väestökirjanpidon sisältämät (demografic information) ja elämäntyyliä koskevat tiedot. (O’Harrow, 2005). Pelkästään minimitason kuvaus ulottuu syvälle henkilöhistoriaan ja on 20 sivua pitkä.

> ”A cousin of mine who works at one of the nation’s largest database companies refused, on privacy grounds, to send me a copy of the information the company had about me. But when she sent a copy of the information about her – including only the public record information and not additional proprietary information (gathered from the commercial sector and law enforcement) – it was more than 20 pages long and included not only a list of all the places she’d lived, but the names of all of her former roommates

> and all of the cars she'd owned. This was the lowest-resolution data image available…" *(Andrejevic, 2007)*

Tiedonhalu ei jää näihin tietoihin, vaan yrityksissä visioidaan jo systemaattisempaa tiedonkeruuta, joka ulottuisi kattavammin koko väestöön. Samalla henkilön tunnistusta halutaan syventää biometrisiin ja DNA-tietoihin perustuvaksi. Tavoitteena on tunnistaa "elävät ja kuolleet, syyttömät ja rikolliset".

> "ChoisePoint officials envision a day when their databases of DNA – something they consider "IDNA" or "the ultimate identifier" – or fingerprints or other biometric banks will be employed routinely to identify everyone, dead and alive, innovent and criminal alike." *(O'Harrow, 2005)*

Erityisesti Britanniassa ja USA:ssa tiedonkeruu on saanut viime vuosikymmenen aikana mittasuhteet, joilla ei ole mitään vertailukohtaa historiassa. Tiedonkeruusta on tullut laajamittaista liiketoimintaa. Lisäksi julkisen ja yksityisen sektorin välille on alkanut tulla uudenlaisia kytköksiä. Julkishallinto on alkanut hyödyntää laajemmin yksityisen sektorin keräämiä tietoja.

Tiedon nopeutuva käsittely ja syvenevä analyysi

Tiedonkeruun ja käytön prosessi on nopeutumassa ja tehostumassa. Tiedon analysointia ja käsittelyä nopeuttavat ensinnäkin tehokkaammat tietokoneet. Esimerkiksi tiedonkeruuyritys Acxiom hyödyntää supertietokoneiden verkostoa (Grid), joka mahdollistaa miljoonien henkilötietojen nopeamman käsittelyn.

> "By 2004, the company had developed its grid supercomputing system, enabling its analysts to do everything faster and with far more depth." *(O'Harrow, 2005)*

Id-numeropohjainen henkilötiedon haettavuus on toisena keskeisenä tekijänä tehostamassa tiedonhakua erittäin laajoista tietokannoista. Esimerkiksi Acxiomissa on tunnistettu se tosiseikka, että identifioiva henkilötunnus avaintietona tekee heidän tietojenkäsittelystään nopeampaa.

> "…the company systematically matches and analyzes the information it collects to create fine-grained portraits about roughly 200 million adults. Every one of them is labelled with a 16-digit code unique to each person to make the processing of their records swifter." *(O'Harrow, 2005)*

ChoisePointin tiedonhallinnan kuvataan olevan tasolla, joissa henkilöiden profilointi, yhteyksien jäljittäminen ja heidän käyttäytymisensä ennakointi on nopeampaa kuin koskaan. Hekin korostavat henkilöön liittyvän tiedonhaun helppoutta, jossa kaikki relevantti tieto haetaan yhdellä hakukomennolla – ilman yhtenäistä tunnistavaa hakuelementtiä se ei olisi mitenkään mahdollista. *(O'Harrow, 2005)*

Tietojen hyödyntämistä tehostavat osaltaan kehittyneemmät tiedonkeruun käytännöt ja analysoinnin menetelmät. Ne tarjoavat monipuolisia ja nopeita mahdollisuuksia tietojen yhdistelylle ja hyödyntämiselle. Esimerkiksi ChoisePointin tiedonkäsittelyssä sovelletaan lisäksi mm. tiedon louhintaa ja visualisointia (geospatial visualization), jossa henkilöön ja häneen sijaintiinsa liittyviä tietoja voidaan tarkastella kartalla (O'Harrow, 2005).

Kehittyneiden tiedonkeruukäytäntöjen ja analyysimenetelmien avulla tietomassoista voidaan jäljittää ennakoimattomia yhteyksiä tai toimintamalleja. Tiedonhallinnan perustana voivat olla kerätyt tiedot (data gathering) tai vaihdetut tiedot (data exchange), joita voidaan edelleen käsitellä tiedonlouhinnan (data mining) menetelmillä. Henkilötiedot voidaan myös liittää yhteen eri lähteistä (data merging), vertailla kohteen tai henkilön yhteensopivuutta muiden kohteiden tai ryhmien tietoihin (data matching) tai tuottaa tiedoista profiileja (pattern recognition). *(Dean, 2005)*

Tiedonlouhinnassa jäljitetään tiedoista merkityksellisiä yhteyksiä. Tietoja analysoimalla voidaan tarkastella niihin liittyviä suhteita, riippuvuuksia, poikkeamia tai kehityskulkuja. Menetelminä ovat mm. yhteyksien, suhteiden ja toimintamallien tunnistus (associations, patterns), luokittelu ja kohderyhmien segmentointi (classification, segmentation) sekä käyttäytymisen ennakointi (predictions). *(Ranjan, 2007)*

Tavoitteena on tunnistaa käyttäytymismalleja ja kohderyhmiä, joita voidaan erotella ennalta määriteltyjen piirteiden, kuten iän, sukupuolen, tulotason ja asuinalueen mukaan. Analyysien pohjalta voidaan kuitenkin tuottaa myös uudenlaisia ryhmiä.

Tulokseksi voi syntyä profiileja, tilannekuvia, ennusteita tai tietoa poikkeamista tai asetettujen rajojen ylityksistä. Pidemmän aikaa säilytetyt tiedot tarjoavat tilaisuuden tarkastella kehityskulkuja tai historiallisia kuvauksia. Myös henkilöhistorialliset analyysit ovat mahdollisia (Evans, 2005).

Tiedon analysoinnille keskeistä on kohdehenkilön tai -ryhmän "käyt-

täytymisen ymmärtäminen”. Tulokset voivat palvella erilaisia tarkoituksia rikostutkinnasta kulutuskäyttäytymiseen ja käyttäytymisen ennakointiin.

> ”When the artificial intelligence comes to understand a customer, that insight doesn’t only have to be applied to criminal activity. It can also be programmed to anticipate when a paycheck is coming in, and when someone is getting a pay raise. Over time it will learn when an individual’s family tends to go on a vacation. It can calibrate how much a bachelor typically spends on Friday nights and where. By analyzing changes in his behaviour, it could also saywhen he has tied a knot.”
>
> *(O’Harrow, 2005)*

Tapahtumavirran ja taustatietojen yhdisteltyyn analyysiin voidaan liittää myös automaattisia hälytyksiä, ilmoituksia tai muita toimenpiteitä. Poikkeamien seuraukset voivat tuntua hyvin nopeasti, olipa kyseessä ylinopeudella ajo liikenteessä tai luottorajan ylitys.

Ubiikinomaista analyysia edustaa puolestaan “reality mining”, jossa hyödynnetään ympäristöstä sensoreilla ja gsm-puhelimilla koottua dataa. Jo paikannustietoihin perustuvalla analyysilla voidaan tehdä päätelmiä paitsi yksittäisen ihmisen liikkeistä, myös heidän tapaamisistaan ihmisistä. Analyyseilla siis tavoitetaan tietoja ihmissuhdeverkostoista ja erilaisten ryhmien sijainnista, liikkumisesta ja kulkureiteistä. Teknologioiden kehittäjien toiveissa on kuitenkin edetä esimerkiksi kännykässä puhutun tulkintaan, jossa puheentunnistamisen teknologioiden avulla voitaisiin tehdä päätelmiä esimerkiksi puhujien mielentilasta.

(Greene, 2008)

Kehittyneessä tiedonhallinnan ympäristössä tiedon arvo muodostuu uudella tavalla. Analysointi asettaa kerätyt tiedot uudenlaisiin kehyksiin. Niissä tiedoista rakentuva kuva riippuu myös tulkintakonteksteista ja vertailutiedoista. Tietojen ostajan tai hyödyntäjän näkökulma ratkaisee sen, miten hän haluaa kohteitaan tulkita.

Ubiikkiympäristön älykkäät teknologiat tulkitsevat kohdehenkilöiden käyttäytymistä yhä tarkemmin ja oppivat siitä. Tiedonkeruu, analyysi ja sen pohjalta käynnistyvät toiminnot voivat vaikuttaa yksilöllisesti. Käyttäjien toimia ja ihmissuhdeverkostoja voidaan niiden avulla ennakoida täsmällisemmin ja heidän aiempien toimiensa perusteella. Ympäristötietoa keräävät analyysit voivat ulottua jopa käyttäjän mielentilan ja terveyden arviointiin. Tietojenkäsittelyprosessista on samalla tulossa nopeampi, automatisoidumpi ja ihmistä kokonaisvaltaisesti arvioiva.

Ubiteknologian kääntöpuolet ja vaikutukset

Teknologiaan kätkeytyneet periaatteet

Tietoteknologian vaikutusten arviointia vaikeuttaa tietoteknologian etiikan tutkijan, Philip Breyn mukaan, teknologian monimutkaisuus, läpinäkymättömyys ja näennäinen neutraalius käyttäjille. Tietoteknologian vaikutukset ja käyttöyhteydet eivät ole ilmeisiä käyttäjälle, koska ne kätkeytyvät monimutkaiseen toiminnallisuuteen. Ne voivat selvitä vasta perehtymällä laajemmin kyseisen laitteiden ja sovellusten toimintaperiaatteisiin ja käyttöyhteyksiin. *(Dodig-Crnkovic, 2006)*

Lawrence Lessigin perusväittämä – koodi on laki – puhuu samasta asiasta, mutta hieman eri näkökulmasta. Teknologian toimintamallit (laki) rakentuvat siitä, mitä se (koodi) mahdollistaa. Teknologia on ymmärrettävissä vain niille, jotka tuntevat sen toimintaperiaatteet eli koodin. Muille käyttäjille koodi on näkymätön. *(Lessig, 2006)*

Lessigin mukaan teknologian toimintaperiaatteet tuottavat uusia järjestyksiä ja arvoja yhteiskuntaan. Ne voivat tulla hyväksytyksi uudenlaisina välttämättömyyksinä. Jos teknologioiden toimintaperiaatteiden annetaan luoda arvoja ja välttämättömyyksiä, niistä tulee ”polittisia” eli vallankäytön välineitä. *(Lessig, 2006)*

Näin on käymässä esimerkiksi käyttäjien tunnistuksen suhteen. Tunnistusteknologia on tuonut mukanaan uudenlaisen tulkinnan käyttäytymisestä, joka ei sinänsä liity teknologiaan. Siitä on tullut välttämättömyys ja itsestäänselvyys. Tunnistuksen yleistyessä toive anonyymista verkkokäytöstä on lisäksi saatu kuulostamaan lähes rikolliselta. Kyse ei ole kuitenkaan siitä, että anonyymia verkkokäyttöä olisi määritelty rikolliseksi tai että tunnistukselle olisi kaikissa yhteyksissä tarvetta.

Koodi pitäisi purkaa, kuten Lessig ehdottaa – eli teknologiaan sisältyvät periaatteet tulisi avata, jotta ymmärrettäisiin, millaisiin toimintaperiaatteisiin yhteiskunnassa ollaan siirtymässä (Lessig, 2006). Tietoteknologian yhteiskunnallisista, poliittisista ja eettisistä vaikutuksista pitäisi siis puhua siten, että teknologioiden mahdolliset käyttöyhteydet ja toiminnallisuudet tulevat ilmi.

Teknologioiden nopea kehitys, ennakoimattomat yhteisvaikutukset, toimintojen ja tietovarastojen piiloutuminen käyttäjiltä sekä palvelujen ja valvonnan kietoutuminen toisiinsa ovat ilmeisiä ubikkiympäristön piirteitä. Ubiikin teknologioihin sisältyvien toimintaperiaatteiden ja käyttöyhteyksien arviointi onkin keskeistä, jotta voitaisiin arvioida, mitä ubiikkiyhteiskunnassa tullaan rakentamaan.

Infrastruktuurivaikutus

Ubiikkiyhteiskunta edellyttää uudenlaista teknologista infrastruktuuria, jonka vaikutukset ovat massiiviset, monialaiset ja laajalle ulottuvat. Yhteiskunnan toiminta ja siinä asiointi rakentuu siinä yhä syvemmin verkkoympäristön varaan, jonka tuntosarvet tunkeutuvat ”kaikkialle”. Ubimaailman toimintamalleilta, tiedonkeruulta ja seurannalta ei voi välttyä.

Ubiikkiyhteiskunta syntyy kerroksittain. Sitä ovat edeltäneet tietoyhteiskunnan kehitysvaiheet, joiden kerroksista ”jokainen on rautaa” – niiden vaikutus yhteiskuntaan on ollut pysyvä ja syvä. Tietoyhteiskunnassa verkon rooli on muuttunut jakelu- ja tiedotuskanavasta vuorovaikutteisten palvelujen ympäristöksi. Siihen kuuluvat laaja käyttäjäkunta, globaali ala, laajat tietovarastot ja monipuoliset palvelut.

Sähköisen asioinnin yleistyminen, tunnistuksen ja paikannuksen laajentaminen ja älykkäämpien ja ympäristöön sulautuvien teknologioiden käyttöönotto ovat loogista jatkoa tälle kehitykselle. Kehityksen ennakoidaan edelleen etenevän tietoteknologian ja bio- ja nanoteknologian yhteen sulautumiseen (konvergenssi), jolloin voitaisiin jo puhua bio- ja fuusioyhteiskunnasta (Mannermaa, 2007). Elävät organismit ja teknologia tulevat sulautumaan yhä enemmän toisiinsa – teknologiaa asennetaan ihmiskehoon ja sillä vaikutetaan eläviin organismeihin.

Sähköinen asiointi muodostaa ubiikkiyhteiskunnalle perustan, jota parhaillaan ollaan rakentamassa. Myös kehityksen myöhemmästä suunnasta on kuitenkin merkkejä jo ubiikkipuheessa (mm. medical implants, TEKES, 2006a, läsnä-älyn sovellutusalueissa mainitaan visiot implanteista, Liikenneministeriö, 2006)

Ubiikkiympäristöllä on infrastruktuurivaikutus. Se muuttaa yhteiskunnan toimintaperiaatteet ja tuo mukanaan laaja-alaisia muutoksia - osin hyvin huomaamattomasti. Ne periaatteet, joiden varassa ubiikkiteknologian palvelut, toiminnallisuudet ja käyttötarkoitukset luodaan, rakentavat uudenlaisen yhteiskunnan. Rakennettua infrastruktuuria ei yleensä pureta ja sen laajamittaiset muutoksetkin voivat olla kalliita. Siksi se, millaiset pelisäännöt ja toimintamallit tätä tehokkaammin tietoa käsittelevää yhteiskuntaa varten rakennetaan, on historiallinen kysymys.

Ontologinen muutos

Ubiikkiteknologian vaikutuksien yhteiskunnassa on ennakoitu muodostuvan käänteentekeviksi, mutta myös käänteisiksi. Greenfield kuvaa teknologista siirtymävaihetta ”paradigman muutoksena”, joka muuttaa maailmankatsomuksemme perusteellisesti. *(Greenfield, 2006)*

Ubiikkiympäristö tuo mukanaan uuden olemisen muodon (”new state of being”), jonka intuitiiviset ja havainnoivat käyttöliittymät tarjoavat. Ubiikkiteknologia aistii, muokkaa ja yhdistelee tietoa ympäristöstään ilman käyttäjän aktiivista toimintaa (Kainulainen, 2005). Asioidessa ja liikkuessa kerättävän tapahtuma- ja tilannetiedon osuus ja sen hyödyntäminen lisääntyy.

Kännykästä voi tulla monitoimilaite, jonka toiminnot laajentuvan puheluista, tekstiviesteistä ja nettiyhteyksistä edelleen etävalvontaan – kuten toisten sijainnin seurantaan (Liikenneministeriö, 2006). Palveluista tulee itsepalveluja – luemme itse lukulaittein ostoksemme ja maksamme ne automaattiin (Rijnbende, 2004). Älykkäät lattiat voisivat seurata liikkumistamme ja valvontakamerat ilmoittaa sallittujen rajojen ylityksemme tiloissa ja välittää niistä tilanteeseen sopivat viestit tai hälytykset eteenpäin (Greenfield, 2006, Halkosaari, 2007).

Ubimaailmassa muuttuu se, millaista ympäristöä pidämme luonnollisena. Muutos on ontologinen. Se vaikuttaa siihen, miten hahmotamme todellisuuden, mitä toimintamalleja pidämme itsestään selvinä ja miten havainnoimme ja reagoimme. Jatkuvasta ja kaikkialle ulottuvasta tietotekniikan havainnoinnista ja tiedonkeruusta ja niiden pohjalta käynnistyvistä toiminnoista tulee uusi olosuhde.

Olemuksellisiin muutoksiin kuuluvat myös uudenlaiset pakot ja ristiriidat. Tiedonkeruuseen ja tunnistamiseen liittyvät velvoitteet ja välineet ovat laajentuneet jo nyt. Teletunnistetietojen kokoamiseen velvoitetaan. Pakollisiksi ovat käytännössä tulleet sirupassit ja monet sirukortit, kuten henkilö-, maksu-, matka- ja kulkukortit. Vaikka kaikki näistä eivät olisi lakisääteisiä, useimmille niistä ei ole toimivia vaihtoehtoja.

Ubiikkiyhteiskunnan pakot laajentuvat todennäköisesti edelleen – niihin voi kuulua esimerkiksi velvollisuus olla kokoaikaisesti seurattavissa tai pitää laitteita jatkuvasti päällä. Seurattavuus, jonka perusteella kansalaiselle on rajat ylittäessä automaattisia seuraamuksia, näyttäisi myös mahdolliselta.

Hyvänä esimerkkinä ovat liikenteen valvontaan liittyvät toimet, joi-

hin on kehitteillä erilaisia ubiikinomaisia menetelmiä. Toimintoihin on yhdistetty mm. RFID-tunnistuksen, GPS- ja satelliittipaikannuksen ja valvontakameraverkostojen tiedonkeruuta. Britanniassa on koottu valvontakameroilla autojen rekisterikilvet tietokannaksi (Savvas, 2006). Amerikkalaisessa autovuokraamossa on tarkkailtu autojen nopeutta GPS-paikannukseen perustuen ja rakennettu sovellus, joka siirtää välittömästi ylinopeudesta sakkomaksun ajajan tililtä. (O'Harrow, 2005). Britanniassa on ehdotettu autojen satelliittivalvontaa, jolloin liikenteeseen ja auton käyttöön liittyviä maksuja voitaisiin kerätä automaattisesti (BBC News, 2005). Myös Suomessa tämän kaltaisia palveluja ehdotetaan toteutettavaksi lähivuosina (Liikenneministeriö, 2006).

Ubimaailman keskeisiin yhteiskunnallisiin jännitteisiin kuuluvat teknologioiden ja tietovarastojen omistukseen, hallintaa ja hyödyntämiseen liittyvien itressien yhteensovittaminen. Kuka kontrolloi ubiikin Internetin kehitystä? Kun eri osapuolten intressit ovat erilaisia, kenen lähtökohdat ja tarpeet asetetaan etusijalle. Miten niiden välille löydetään tasapaino?

Matkasta kohden ubiikkiyhteiskuntaa ei tule helppoa. Sen ennakoidaankin aiheuttavan yhteiskunnassa ”mullistuksen, joka on kaikkia aikaisempia syvempi ja väkivaltaisempi”. (Liikenneministeriö, 2006). Ubiikki ei tuo yhteiskuntaan vain uusia olosuhteita, vaan myös uusia toimintaperiaatteita, joiden vaikutukset ovat tuntuvat.

Avoimuudesta hallintaan

> *”Cyberspace is regulated by its code, and that code is changing. Its regulation is its code, and its code is changing.”*
>
> *- Lawrence Lessig*

Syntyessään 1990-luvulla Internet-verkon avoimuutta pidettiin ainutlaatuisena. Verkko antoi virtuaalisen tilan ja ympäristön, jossa kaikki se, mikä mielikuvitukselle ja verkon välineille oli mahdollista, saatettiin toteuttaa. Verkko tarjosi mahdollisuuden irrottautua fyysisen ympäristön rajoituksista ja uudenlaisen tilan viestinnälle ja verkostoitumiselle.

Käsitys vapaasta ja säätelemättömästä Internetistä on sittemmin muuttunut. Jo 1990-luvun lopulta on ennakoitu, että verkosta tulee lisääntyvässä määrin kontrolloitu ja säädelty ympäristö.

> ”We have been as welcoming and joyous about the Net as the earthlings were about the aliens in Independence Day; we have accepted its growth in our lives without questioning its own free-

> dom. But at some point, we too will come to see a potential threat. We will see that cyberspace does not guarantee its own freedom but instead carries an extraordinary potential of control.”
>
> *(Lessig, 2006)*

Lessigin mukaan verkkomaailman luonteen muutokseen vaikuttavat erityisesti sähköiseen identiteettiin liittyvät teknologiat. Kontrollin välineet rakentuvat pinnan alla tavalla, joka eivät näy käyttäjälle. Kontrolli tulee sisäänrakennettuna identiteetin hallinnan teknologioihin, niin kuin Troijan hevonen.

> ”If anything is certain, it is that an architecture of identity will develop on the Net – and thereby fundamentally transform its regulability.” *(Lessig, 2006)*

Kehitykseen vaikuttavia tekijöitä on nähty eri tavoin. Vernon Vinge esitti jo 1996, että tulossa verkkoympäristö, jossa hienojakoiset hajautetut järjestelmät tukevat arkielämän toimia, mutta myös keräävät tietoa hallitukselle ja ovat hallituksen ohjauksessa. Vingen varhainen pelko verkkomaailmaan rakentuvasta kontrollista kuvaa myös sitä, miten keskittynyt teknologioiden hallinta voisi johtaa äärimmäisen säädeltyyn yhteiskuntaan.

> ”Our digital selves - and increasingly, our physical selves, would live in a world of perfect regulation, and the architecture of this distributed computing – what we today call Internet and its successors – would make that regulatory perfection possible.”
>
> *(Lessig, 2006)*

Tom Maddox on myöhemmin arvioinut, että hallinnan ja säätelyn laajentuminen ei lisäänny yksinomaan julkishallinnon myötävaikutuksella, vaan yksityisen sektorin ja julkishallinnon yhteisten intressien tuloksena. Yksityisellä sektorilla kehitetään välineet ja hallinnon sektorilla kontrollin muodot. *(Lessig, 2006)*

Kontrollin ja sensuurin muodot verkossa näyttäisivät olevan etenemässä kaikilla edellä kuvatuilla tavoilla. Kontrolli verkkomaailmassa on lisääntynyt yksityisten ja julkisten tahojen vaikutuksesta ja osin heidän yhteistoimintansa kautta. Samoin verkkomaailman arkkitehtuurin muutos, jonka perustan luovat tunnistaminen ja sähköinen identiteetti, on etenemässä nopeasti.

Valvonnan arkkitehtuuri

> *”If you create a data surveillance system, someone will find other uses for it. It almost always happens.”*
>
> *- Robert O’Harrow*

Valvonnan rakentumisen verkossa on katsottu edellyttävän kolmea keskeistä käytäntöä: kattavia henkilötietojärjestelmiä, kehittyneitä tietoverkkoja ja yleisesti sovellettavaa tunnistusratkaisua (Heinonen, 2001). Kehitys on edennyt askel askeleelta tähän suuntaan, mutta ubimaailman teknologiat tehostavat sen vaikutuksia. Ne laajentavat henkilöön liittyvien tietojen alaa, syventävät tiedonkeruuta tapahtuma- ja tilannetietoihin ja nopeuttavat tietojen analysointia ja käyttöä. Tunnistuksen ja paikannuksen kaikkialle ulottuvat liitännät tekevät siitä aukottoman.

Ubimaailman suurimmat uhkakuvat ovat sisäänrakennettuina ubiteknologian arkkitehtuurissa, joka on luonteeltaan massojen valvontateknologiaa. Sen välineissä yhdistyvät valvonnan, logistiikan hallinnan, tunnistamisen, paikantamisen ja tiedonhallinnan työvälineet. Ubiteknologian välineillä rakennetaan yhteiskuntaan paitsi uudenlaisten palvelujen ympäristö, myös ennennäkemättömän tehokas valvonnan ja hallinnan infrastruktuuri.

> ”Kun Internet-käyttäytymisen tai mediakulutuksen seuranta tarjoaa vain kapean tirkistysluukun ihmisten arkeen, muodostaa ubiteknologia todellisen panoptikonin, jonka katseelta ei jää mikään havaitsematta.” *(Liikenneministeriö, 2006)*

Greenfield kuvaa ubiteknologiaa jopa ihanteelliseksi laajojen väestöryhmien valvonnan välineeksi ja toimintamalliksi.

> ”At the most basic level, it would be difficult to imagine a technology more suited to monitoring a population than one sutured together from RFID, GPS, networked biometric and other sensors, and relational databases; I’d even argue that everyware redefines not merely computing but surveillance as well.”
>
> *(Greenfield, 2006)*

Ubimaailmassa on sekä hyödyllisiä, että valvontayhteiskunnan kehittymistä tukevia riskisovelluksia. Hyöty- ja riskisovellusten mittasuhteita on vaikea arvioida, mutta niiden vaikutuksia ja yhteyksiä on tunnistettavissa. Ne näkyvät monessa muodossa, kuten yritystoiminnan luonteessa, tiedonkeruun ja tunnistusteknologioiden käytännöissä sekä palvelujen omistuksen ja hallinnan rakenteissa.

Tietoteknologian käänteisvaikutuksista yritysten toiminnassa on esimerkkejä jo verkkokehityksen aiemmista vaiheista. Yritysten liiketoimin-

taperiaatteet ovat saattaneet muuttua asiakaskunnan mukaan, mikä on voinut muuttaa tuotteen luonnetta ja käyttötarkoituksia käänteiseen suuntaan.

Varhaisin esimerkki näistä kuvaa valvontasovellusten kehitystä. 1995 Baijerissa haluttiin yksiselitteisesti estää pornon tarjonta verkossa. CompuServe kehitti tähän tarkoitukseen filtterointiohjelman. Ohjelmaa kehitettiin edelleen selvittämään verkkoympäristöstä, kuka on käyttäjä, mitä hän tekee ja missä hän toimii. CompuServen palvelu loi käytännössä lähtökohdat ja mallit sille, miten seuranta ja valvonta Internetissä jatkossa toimi.

(Lessig, 2006)

Tehokkaampaa tietoturvaa tarjoavat yritykset ovat toimineet myös käänteisten palvelujen tarjoajina. Network Associates arvosteli alkuaan kryptaukseen liittyvää säätelyä. Sittemmin sama yritys on tarjonnut yrityksille välineitä, joilla kryptausta hallitaan ja avataan. Cisco toi tarjolle reitittimiä, joiden avulla Internet liikennettä voisi kryptata. Nyt yritys tarjoaa reitittimiä, joiden hallinnassa voidaan valita, sallitaanko kryptausta vai ei.

(Lessig, 2006)

Useat tunnetuimmista kansainvälisistä tietoteknologiayrityksistä ja hakupalveluiden tuottajista ovat rakentaneet sovelluksia valvonnan ja kontrollin tarkoituksiin. Valvonnan ja turvallisuuden sovellukset ovat voineet jopa eriytyä omaksi liiketoiminnan alueekseen. Esimerkiksi Microsoft, Google ja Yahoo, ovat avustaneet viranomaisia kontrollitoimissa (Mills, 2006).

Ubiikkiteknologian, samoin kuin muut informaatioalan teknologioiden taustalta löytyvät myös puolustushallinnon sovellukset. USA:ssa DARPA (Defence Advanced Research Projects Agency) toimii tunnetusti älytuotteisiin liittyvän tutkimuksen rahoittajana (TEKES, Suomen Akatemia, 2006). NSA (National Security Agency) on ollut myös rahoittamassa laaja-alaisia tiedonkeruuhankkeita, jotka ulottuvat verkkosisältöihin ja yhteisöllisiin palveluihin (”the mass harvesting of the information people post about themselves on social networks”) (Andrejevic, 2007). Ubiteknologioita hyödyntävät sotilaalliset ja turvallisuusvalvonnan sovellukset ovat jo nyt pitkälle kehittyneitä ja niiden käyttötarkoituksiin hyödynnettävät tietovarastot massiivisia.

Ubiikkiteknologian pitäminen arvoneutraalina on arveluttavaa, johtuen sen luonteesta, käyttöyhteyksistä ja kytköksistä. Jos valvontayhteiskunnan kehittymiseen halutaan puuttua, näiden yhteyksien olemassaolo on tunnistettava ja niiden vaikutuksia ymmärrettävä. Emme voi olla varmoja, ettei hyötypalveluja tuottavilla teknologioilla rakenneta myös kansalaisille ja yhteiskunnalle ongelmallisia palveluja, joita voi tuottaa jopa sama yritys.

Verkossa liikkumisesta jää jäljet

Tiedonkeruu on kätkeytymässä ubiikinomaiseksi asioinnin oheistoiminnoksi lähes kaikkialla arkisessa ympäristössä. Tapahtumatieto syntyy korttia vilauttamalla joukkoliikenteessä liikkuessa, telemarkkinoijan soittaessa, autoa tai asuntoa vuokratessa ja asioinnissa kaupan kassoilla tai verkossa (O'Harrow, 2005).

Verkossa tiedonkeruun käytännöt ovat muuttuneet oleellisesti siitä, mitä ne ovat olleet fyysisessä ympäristössä. Tiedonkeruu kätkeytyy toimintoihin, eikä se näy käyttäjälle. Käytännössä käyttäjän jokainen tiedonhaku, kirjoitus ja asiointitoiminto sekä hänen kontaktinsa verkossa voivat päätyä palveluntarjoajien tai muiden tiedonkerräjien haaviin.

> ”Whereas peer-to-peer monitoring in traditional communities is symmetrical and relatively transparent, the same cannot be said, in many cases, of networked, distributed monitoring. Background-check software, googling and even sites like Facebook can be used without knowledge of those about whom information is being gathered.” *(Andrejevic, 2007)*

Verkkoa ei voi käyttää jälkiä jättämättä. Jo yhteyden avaaminen kirjautuu teletunnistetietoihin, jotka telepalvelun tarjoajat keräävät kaikilta asiakkailtaan. Verkossa liikkumista, tiedonhakua ja palveluissa asiointia seurataan sen lisäksi monella muulla tavalla.

Verkossa liikkuessaan käyttäjä jättää tyypillisesti tietonsa ip-osoitteestaan, selaimestaan, käyttöjärjestelmästä, kielestä ja mahdollisesti käytössä olevista lisäohjelmista. Nämä tiedot voi kerätä mm. tietoliikennepalvelun tarjoaja, palvelimen ylläpitäjä tai sovelluksen hallinnoija. Jos käyttäjä avaa tietyn verkkosivun, on teoriassa jokaisella laitteella, jonka läpi pyyntö kulkee, mahdollisuus tallentaa käyttäjän tietoja lokeihinsa. Tyypillisesti pyyntö kulkee verkossa läpi useiden palomuurien, reitittimien läpi kohden varsinaista palvelinta, johon otetaan yhteys. Laitteiden omistajia ei voi tietää, eivätkä he välttämättä kerro, millaista tietoa he keräävät.

(Järvinen & Saarelainen, 2007)

Tietoja palveluissa liikkumisesta voidaan kerätä lokitiedoista tai ns. piparin (cookie) avulla, joiden käyttö on vakiintunut verkossa. Verkossa liikkuu jatkuvasti myös käyttäjän havaitsematta erilaisia tiedonkeruuohjelmia. Googlen tiedetään keräävän tiedot jokaisesta hausta, hakusanoista ja laitteesta, josta haku tehdään (Andrejevic, 2007, Lessig, 2006). Erilaisia sovelluksia on kehitetty myös käyttäjien ihmissuhdeverkostojen selvittämiseksi ja ryhmien organisoitumisen seuraamiseksi (Andrejevic, 2007).

Suurin osa verkossa kirjoitetusta poimiutuu Googlen indekseihin ja on haettavissa, vaikka kirjoittaessaan olisi esimerkiksi rekisteröitynyt suljettuun keskusteluryhmään. Verkkopalveluihin rekisteröityminen tai tunnistettu asiointi kokoaa tietoja vielä varmemmin palvelun tarjoajalle. Verkko ei ole yksityinen, vaan hyvin julkinen media nykymuodossaan.

Vain harvoin kansalaisella on mahdollisuus kieltää itseään koskevien tietojen keruu ja luovuttaminen eteenpäin tinkimättä niistä palveluista, joita haluaa käyttää. Jo rekisteröityminen tai palvelun käyttöön saaminen voi edellyttää lupaa tietojen luovutukseen. Kytkykauppa palvelujen ja tietojen luovutuksen välillä ei ole tavatonta. Käyttäjä tekee vaihtokaupan yksityisyydestään sallimalla tiedonkeruun palveluja vastaan.

Erilaisista tilanteista kerättyjä tietoja voidaan yhdistellä ja viedä tietokantoihin. Tietoja voidaan kuitenkin yhdistellä myös käyttäjien antamiin yhteystietoihin, jotka hän on antanut esimerkiksi rekisteröinnin, kyselyihin tai tutkimuksiin vastaamisen yhteydessä. Palveluntarjoajat käyttävät näitä tietoja esimerkiksi tilastointiin ja palvelujen kehittämiseen.

(Järvinen & Saarelainen, 2007)

Tiedonkeruuyrityksien käytännöt ovat toisenlaisia. Heillä voi olla hallussaan tietoja, jotka on voitu ostaa, vaihtaa tai koota erilaisista julkisista ja maksullisista lähteistä. Tiedot voivat olla peräisin verkosta tai sen ulkopuolelta. Yritykset voivat yhdistellä rekisteröintitietoa, verkossa, palvelussa ja liikenteessä asioinnista kerääntyneitä tapahtumatietoja sekä kysely- ja tutkimustietoa.

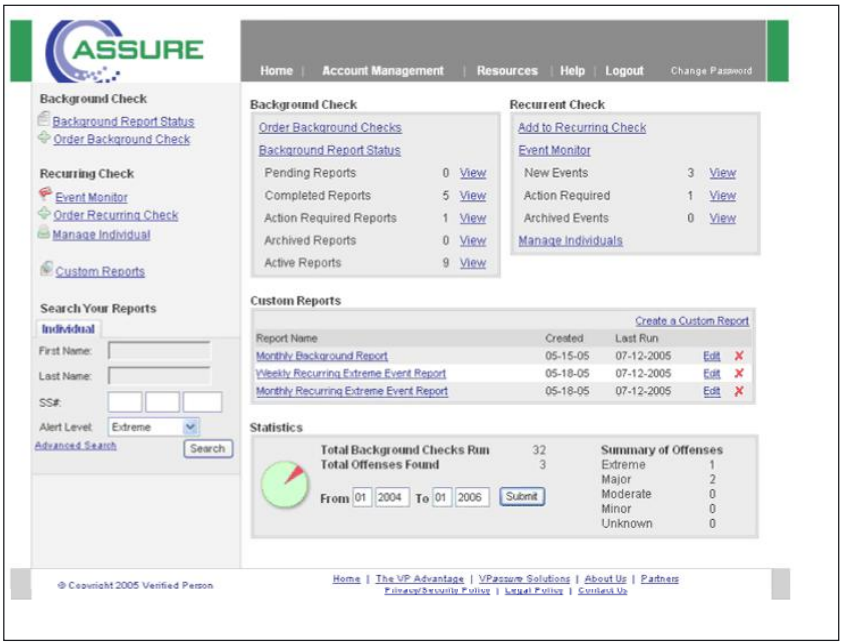
Henkilöön liittyvillä tiedoilla on monenlaisia käyttöjä. Yksityisten yritysten käyttötarkoituksina ovat olleet etenkin myynnin edistäminen ja tappioiden minimointi, tuote- ja palvelutarjonnan kohdentaminen ja personointi, investointipäätösten arviointi, petoksilta suojautuminen ja luottoihin liittyvien riskien hallinta. Julkisella sektorilla kohteena ovat olleet mm. riskien hallinta, rikostutkinta ja aluepoliittinen suunnittelu.

(Lace, 2005)

Tiedonkeruuyritysten asiakaskunta on laajentunut nopeasti 2000-luvulla, etenkin USA:ssa. Siihen kuuluvat nyt rinnakkain julkishallinto, yritykset ja yksittäiset kuluttajat.

Yksityishenkilöille tarjotaan taustaselvityksiä jopa pizzakuskeista, jotta kuluttaja voisi näiden tietojen pohjalta tilata turvallisimman pizzan (O'Harrow, 2005). Kuluttajille tarjolla oleva taustatieto on myös hämmästyttävän laaja-alaista. Se voi kattaa esimerkiksi sosiaaliturva-, vero-, rangaistus- ja puhelutiedot (Krim, 2005). Työnantajille tarjolla

on esimerkiksi jatkuvaa työntekijän taustojen seurantaa (Business week, 2006).



Kuvio 1. Assure-palvelun henkilön seurantaraportti

Tiedonkeruun menetelmät ja yhteydet eivät ole yleisessä tiedossa. Tietovirrat ovat organisaatioiden välisiä ja tietojen käyttö ei välttämättä näy käyttäjille. Ubiikkimaailmassa näkyvyys on vielä heikompi, kun tiedonkeruu ja sen käytöt piiloutuvat käyttäjältä arkiseen ympäristöön. Kokonaiskuvan ymmärtäminen edellyttäisikin käyttäjältä tiedonkeruuseen, vaihtoon ja hyödyntämiseen liittyvien käytäntöjen ja teknologioiden tuntemista.

Tiedonkeruusta valvontainfrastruktuuriksi

2000-luvun puoleen väliin mennessä julkishallinnon ja yksityisen sektorin välinen yhteistyö on USA:ssa edelleen kehittynyt muotoon, jota on kuvattu valvontainfrastruktuuriksi. Tämä näkyy julkishallinnon ja yrityssektorin kytköksinä erityisesti tiedonkeruussa, joihin liittyvät erityisesti erilaiset kontrollin ja valvonnan tarpeet.

> ”Almost everyone you do business with collected information about you, sold it to someone else, or sifted it for their mercantile ends…By now those bargains are being transformed, usually without your input, into a public-private security infrastructure, the likes of which the world has never seen.” *(O’Harrow, 2005)*

WTC:n terrori-isku 11.9.2001 muodosti käännekohdan, jonka jälkeen valvonnan, tiedonhallinnan, tiedonhaun ja älykkäiden teknologioiden yhdistely ja kehittäminen alkoi saada uutta vauhtia. Sovellukset puolustuksen, turvallisuuden ja valvonnan tarpeisiin lisääntyivät. Tiedonhallinnan ja valvonnan intressit ja teknologiat kietoutuivat uudessa vaiheessa nopeasti yhteen. Valvonnasta ja tiedonkeruusta, etenkin julkishallinnon tarpeisiin, tuli tuottava ja kasvava liiketoiminnan alue. *(O’Harrow, 2005)*

Luotettavuuden arviointi ja henkilötietojen seulonta siirtyi maan rajoilta moniin muihin yhteyksiin. Taustaselvityksiä tehdään yhä laajemmin esimerkiksi työnhaussa, luottojen ja vakuutusten valvonnassa tai asuntojen ja autojen vuokrauksessa. Valvonnan ja tiedonhallinnan edistyneimmät yhdistelmät löytyvät nykyisellään kasinoista, joissa pelurien identiteetti ja taustatiedot tulevat tarkistetuiksi jo kättelyssä.
(O’Harrow, 2005)

Turvallisuustarkoituksiin liittyvä tiedonkeruusta on tullut monille yrityksille myös kokonaan oma liiketoiminnan alueensa. Esimerkiksi ChoisePoint, suurin yhdysvaltalainen tiedonkeruuyritys, joka toimii yhteistyössä julkishallinnon kanssa, on panostanut vahvasti turvallisuuden sovelluksiin. Laaja ja kasvava osa myynnistä tulee ”riskien lieventämisestä”, jota varten tarjotaan taustaselvityksiä, työntekijöiden seulontaa sekä erilaisia taustatietoja. Näiden hankkijoina ovat esimerkiksi poliisi, viranomaiset ja tiedusteluorganisaatiot. *(O’Harrow, 2005)*

Choise Pointin liiketoiminnasta on muun ohessa tullut maailman suurin turvallisuusoperaatio. Tiedonkeruun ja tiedustelun intressit kulkevat siinä rinta rinnan. Tehokkaat tiedonhallinnan menetelmät tekevät siitä myös nopeaa.

> ”By 2004, it had become perhaps the world largest private intelligence operation. Its services mirrored what good intelligence analysts do, only ChoisePoint identifies the patterns and links and potential tendencies much faster, and with a sweep that would make James Bond’s colleagues envious.” *(O’Harrow, 2005)*

Acxiom, toinen merkittävä yhdysvaltalainen tiedonkeruuyritys, tunnetaan myös toiminnastaan julkishallinnon valvontajärjestelmien kehityksen tukijana.

> ”And since September 11, 2001, Axciom has offered its technical know-how and raw material…to some of the largest surveillance and screening systems ever devised by the U.S. government.”
> *(O’Harrow, 2005)*

Tiedon keruun laajuus ja sen käyttötarkoitukset turvallisuustarkoituksiin eivät kuitenkaan kaipaa laajempaa julkisuutta. Esimerkiksi ChoisePoint suuntautuu matalalla profiililla markkinointiin ja tiedotukseen laajemmille yleisöille.

> ”Company officials make no effort to advertise to the general public what the company is becoming. They worry the reality would scare people. They also don’t think that most people would believe in them.” *(O’Harrow, 2005)*

On mahdollista, että amerikkalaisesta tiedonkeruun valvontainfrastruktuurista nousevat laajentuvat laineet. Patriot Act -lainsäädännön hyväksymisen jälkeen DARPA käynnisti globaalin valvontajärjestelmän kehittämisen (O’Harrow, 2005). Se, millaisia liitäntöjä sillä olisi tiedonkeruun ja analysoinnin virtoihin, jotka yritysten ja julkisten toimijoiden käsien kautta kulkevat, jää arvailtavaksi.

Verkon uusi järjestys on identiteetti

Sähköinen identiteetti ja tunnistaminen ovat keskeisiä tulevaisuuden verkkomaailman kontrollin välineitä, joita voidaan jopa pitää verkkoa organisoivana paradigma.

> ”If everything is a distributed network there is no hierarchy. In a distributed network there is only one logical organizing paradigm and it is identity. It is the only way you can maintain any control or order over anything,” (Eric Norlin, IDG) *(Fontana, 2006)*

Lessig on ennakoinut kehityskulun täsmälleen samansuuntaisesti. Hän näkee käyttäjien tunnistuksen avulla verkkoon rakentuvan kerroksen, joka luo mahdollisuudet ennennäkemättömiin kontrollin välineisiin. Ne muuttaisivat pinnan alta koko Internetin luonteen. *(Lessig, 2006)*

Identiteetin hallinnan ja tunnistuksen käytäntöihin sisältyy siis kääntöpuoli. Käyttäjien tunnistamisella ei edistetä vain tietoturvaa, vaan se voi yhdistyä tietoympäristöihin, joihin kuuluvat tiedonkeruu, tietovarastojen yhteiskäyttö, tietojen vaihto ja niiden ubiikinomainen hyödyntäminen. Tunnistuskäytännöt eivät takaa tietosuojaa, vaan voivat purkaa sen. Kun tunnistustiedot liitetään tietokantoihin ja tietovarastot laajentuvat keräämään tapahtumatietoa ja niiden käyttöä yhdistellään, jäljet

käyttäjien viestinnästä, liikkeistä ja asioinnista tulevat itse asiassa yhä tarkemmin ja laajemmin seurattaviksi.

Ubiikkiympäristössä älykkäämmät laitteet ja sovellukset antaisivat edelleen mahdollisuuden reagoida käyttäjien toimiin lähes reaaliaikaisesti. Näin toimisivat esimerkiksi ubiikinomaiset liikenteen valvonnan muodot, kuten liikenteen seuranta ja siihen liittyvien maksujen kerääminen (Rainio, 2005).

Digitaalista allekirjoitusta ja sen leviämistä käyttöön verkkomaailman ”passiksi”, pidetään tunnistusteknologioiden merkittävimpänä yksityisyyttä uhkaavana osana. Sen laajempi käyttöönotto antaisi mahdollisuudet yhdistellä tunnistustietoja eri tietojärjestelmistä ja kutistaa anonymiteetin ja yksityisyyden alaa. Digitaalisesta allekirjoituksesta tulisi käyttäjille yleisavain verkkoon, mutta myös palvelujen hallinnoijille yleisavain henkilöön liittyviin tietoihin eri tietojärjestelmissä.

(Heinonen, 2001)

Tunnistuskäytäntöjen kääntöpuolet näkyvät myös muualla sähköisessä asioinnissa. Kyse ei ole vain tunnistamisesta ja asioinnista, vaan myös tiedonkeruusta ja varastoinnista. Sähköinen asiointi ei mahdollista vain asiointia, vaan myös kokoaa ja säilyttää henkilöön liittyvät tapahtumatiedot ja asiointihistorian. Sähköisen asioinnin tavoitteisiin kuuluu kansalaisen asiointitili, johon kootaan hänen asiointitietonsa ja asiointihistoriansa verkossa (Nivala, 2006). Verkkoasioinnissa kansalaisesta rekisteröitävän tiedon määrä moninkertaistuu, pysyy muistissa ja siitä muodostuu sähköisiä elämänkertoja.

Identiteetin hallinnan kehitys on pinnan alla syventymässä ja yhdentymässä myös kansainvälisesti. Kansallista kehitystyötä ja kansainvälistä taustatyötä hallinnollisesti ja teknologisesti yhteensopivien identiteettijärjestelmien kehittämiseksi on tehty jo vuosia (Arora, 2007, Gaston, 2007). Kyse ei ole vain sähköisistä henkilökorteista, passeista ja viisumeista, vaan henkilötietoja täydentämään kaivataan myös uudenlaisia tunnistetietoja, kuten biometrisia tai kasvo- ja sormenjälkitunnisteita.

Syvenevä tunnistus, laajentuva tiedonkeruu ja tietojen ubiikinomainen valvontakäyttö näyttävät myös etenevän samanaikaisesti. Viranomaiset eri maissa ovat viime vuosina käynnistäneet satoja hankkeita, joiden tavoitteena on tarkempi käyttäjien tunnistaminen (erityisesti biometrisin menetelmin), DNA-tietokantojen kehittäminen sekä reaaliaikainen viestinnän seuranta ja valvonta (Privacy International, 2007).

Tunnistamiselta välttyminen tulee koko ajan hankalammaksi, mutta

sen eteneminen hävittää verkosta vähitellen anonyymin tilan. Eräs verkon anonyymin käytön keinoista on ollut kryptaus (encrypting). Tämä käytäntö tehdään lähtökohtaisesti mahdottomaksi jo Internet -protokollien tasolla. IPv6 tulee merkitsemään kaikkeen tietoon sen alkuperäisen osoitteen, jota ei voida muuttaa. Internetin liikenteestä tulisi sen rakenteiden pakottamana läpinäkyvää.

> ”…marks each packet with an encryption key that cannot be altered or forged, thus securely identifying the packet’s origin. This authentication function can identify every sender and receiver of information over the Internet, thus making it nearly impossible for the people to remain anonymous on the Internet.”
>
> *(Lessig, 2006)*

Yhtälö ei näytä lupaavalta. Käyttäjien tarkemman tunnistamisen ja sen kansainvälisesti yhdentyvien toimintaperiaatteiden kehityskulkuun limittyy huoli verkkoon laaja-alaisesti ulottuvasta valvonnasta.

> “Arguably, the identity management approaches by government and the private sector represent two sides of the same coin: that is, they both aim to provide security and convenience, with authentication of the individual being the crux. What is striking is the degree to which the international rules and technology may combine to enable comprehensive surveillance in the networked world.” *(Rundle & Laurie, 2005)*

Laajeneva tunnistus takaa sen, että verkossa asioivan jokaisesta askeleesta jää jälki, joka tulee haluttaessa tunnistetuksi. Tunnistuksen, tiedonkeruun, tietovarastojen yhteiskäytön, kansainvälisen yhdentymisen ja ubiikinomaisen hyödyntämisen yhteisvaikutukset voivat olla ennakoimattomat. Asioinnin, liikkumisen ja viestinnän kontrolli kasvaa ennennäkemättömiin mittasuhteisiin näiden käytäntöjen laajentumisen ja yhdentymisen myötä.

Tunkeutuminen arkeen ja kehoon

Ubiikin tiedonhallinta tulee yhä lähemmäksi arkea ja kehoa. Muutosta kuvataan myös ihmiskunnan seuraavaksi siirtomaavallan muodoksi, joka ei tällä kertaa etsiydy kaukaisiin maihin, vaan tulee aiempaa lähemmäksi ihmistä. Ubiikkiteknologia valjastaa automaation hallintaan koko ihmisen arkisen toimintaympäristön.

> ”The project of everyware is nothing less than the colonization of everyday life by information technology.”
>
> *(Greenfield, 2006)*

Ubiikin kosketuspinta ei jää vain arkisen ympäristön esineisiin ja toimiin ja niistä kerättävään tietoon, vaan se koskettaa myös kehoa. Uuden siirtomaavallan piiriin kuuluvat myös kehomme ja ruumiinosamme. Ne purkavat rajaa koneen ja ihmisen välillä.

> ”…on runsaasti perusteita väittää, että ihmisen biologinen ruumis on rajaseutu, jota valloitetaan tieteen ja tekniikan viimeisillä keksinnöillä…Ihmisen ja koneen välinen raja on siis tältäkin osin hämärtymässä.” *(Inkinen, 2004)*

Kehoa lähemmäksi tulevat jo ympäristöstä kuvaa, ääntä, paikannustietoa, biometrista ja sensorien keräämää tietoa yhdistelevät sovellukset (Wactlar et.al., 2003). Niitä voidaan käyttää henkilön käyttäytymiseen, kokemuksiin ja fyysisiin tiloihin liittyvän tiedon keräämiseen. Tietojen pohjalta voidaan tehdä päätelmiä esimerkiksi henkilöiden tunnetiloista ja fyysisestä tai mielenterveydestä. Teknologian sovelluksia on kehitteillä terveydenhoidon tarpeisiin, mutta samankaltaista teknologiaa suunnitellaan myös valvontaan. Microsoft on esimerkiksi patentoimassa menetelmää, joka verkkokameran ja langattomien sensorien avulla voisi seurata työntekijän stressitasoa, keskittymistä, ilmeitä ja liikkeitä (Olsson, 2008).

Kehoon puuttumisen ydinteknologiaa on RFID eli kehoon erilaisiin tarkoituksiin asennetut muistisirut ja niiden hyödyntäminen. Kehoon asennettuja siruja voidaan käyttää henkilön tunnistamiseen, paikantamiseen ja seurantaan. Biosiruilla voidaan myös vaikuttaa elintoimintoihin ja seurata niitä tai pyrkiä normaalin suorituskyvyn parantamiseen (esim. Department of Commerce, National Science Foundation, 2002, Nsanze, 2004).

Turvallisuuden ja valvonnan sovellukset ovat etenemässä myös kehoon istutettujen sirujen käytössä. Britanniassa on hiljattain ehdotettu ihon alaista sirutusta vankien valvonnan menetelmäksi (Brady, 2008). Mitä sitten tarkoittaisi muiden kansalaisten sirutus? Kehitykseen liittyviä uhkia on USA:ssa pidetty niin vakavina, että joissakin osavaltioissa on viety läpi laki, jolla ihmisten pakkosirutukset kielletään (http://www.anti-chips.com).

Keho voi tarvita myös uudenlaista säteilyturvaa. Ubiikkiympäristössä ihmiseen vaikuttavat yhä useammin uudentyyppiset langattomat ja elektromagneettiset ympäristöt, joiden säteet läpäisevät kehon. Näiden vaikutuksia ei tunneta. Kuitenkin jo suunnittelussa otaksutaan, että hypersensitiivisten tai sähköallergisten henkilöiden reagointi olisi syytä ottaa vakavasti. Reaktiot voivat viitata yleisempiin terveyshaittoihin, joita tämänkaltaiset ympäristöt tuovat mukanaan. *(TEKES, 2006a)*

Ubiikkiteknologia on kehoa lähimmäksi tuleva teknologia, jota historiassa olemme nähneet. Se puuttuu kehon hallintaan ja intiimiin alueeseen. Oikeudellisessa mielessä siihen liittyy kysymys siitä, onko ihmisellä itsemääräämisoikeus kehoonsa, siihen kytkettäviin laitteisiin ja keholle turvalliseen ympäristöön?

Kenen käsissä on verkon kontrolli?

Lessigin mukaan verkkomaailma (cyberspace) rakentuu lakien, sosiaalisten normien, markkinavoimien ja teknologisen arkkitehtuurin intressien vaikutuksesta (Lessig, 2006). Kehitystä ohjailevat siis teknologian toimintaperiaatteet, markkinat, lainsäädäntö sekä se, mitä kuluttajat ja yhteiskunta ovat valmiita ottamaan vastaan. Teknologian käyttöönoton vaikutukset riippuvat siitä, kenen reunaehtoja, etuja ja tarpeita painotetaan.

Ubiikkiyhteiskunnan yksityisiä ja kaupallisia intressejä edustavat esimerkiksi markkinatutkimus- ja tiedonkeruuyritykset, mediat, tietoliikenneyritykset, laitteiden ja sovellusten valmistajat.

Julkisen vallan intressinä on toimia vastavoimana markkinoille, mutta luoda myös sille suotuisia olosuhteita. Keinoina ovat mm. kilpailun ja innovaatioiden edistäminen sekä monopolien ja suhteettomien markkinaetujen rajoittaminen. Julkinen etu edellyttää lisäksi julkishallinnon tehokasta toimintaa.

Kansalaisten edun tulisi toteutua myös julkisen sektorin toimien kautta. Sen olisi varmistettava ubiikkiyhteiskunnassakin oikeusvaltion perusarvojen, kuten demokratian ja kansalaisten perusoikeuksien toimivuus. Näitä tulisi edistää lainsäädännössä ja julkishallinnon toimintamalleissa.

Kansalaiset voivat myös itse valvoa etujaan äänestämällä, osallistumalla julkiseen keskusteluun ja vaikuttamalla päätöksentekijöiden toimiin suoraan tai eturyhmien kautta. He tekevät valintoja myös kuluttajina, jos heillä on aitoja vaihtoehtoja. Internet-aikana yhteisölliset ja kansalaispalvelut ovat myös avanneet kansalaisille entistä laajemmat vaikuttamisen kanavat verkossa.

Ubiikkimaailman käytännöissä intressitahojen vaikutusvallan nähdään myös hajautuvan. Mannermaa puhuu valvonnan hajautumisesta käsitteellä ”jokuveli”. Hänen mukaansa ubiikkimaailmassa eletään akvaarioelämää, jossa kuka tahansa (”jokuveli”) voi seurata toistaan tai hyödyntää toisesta kerättyä tietoa (Mannermaa, 2007). Esimerkiksi USA:ssa maksua vastaan julkisesti tarjolla olevat seuranta- ja paikannuspalvelut

voisivat olla eräs ”jokuveli”-ilmiön muoto. Verkko olisi sellaisena joka suuntaan läpinäkyvä.

Jokuveli-skenaarion ja läpinäkyvän ubiikkimaailman toteutuminen ei näytä kaikilta osin todennäköiseltä. Kaupallisilla toimijoilla on toki intressejä myydä tietoja ja teknologioita kaikille maksaville tahoille. Julkisilla toimijoilla voi puolestaan olla avoimuuteen liittyviä velvoitteita.

Toisaalta verkkoympäristön teknologiat, palvelut, tietovarastot ja kontrollin muodot eivät ole edes nyt tasaisesti jakautuneet. Kaikki niistä eivät myöskään ole demokraattisen valvonnan alaisina, eikä niihin sisältyvistä tiedoista, toiminnoista ja tietojen käyttötarkoituksista ole käsitystä. Jos läpinäkyvyydellä tarkoitetaan tietoihin tai palveluun pääsyä tai teknologian saatavuutta markkinoilla, käsitys jää pinnalliseksi. Ubiikkiympäristössä kyse on myös mittasuhteista ja niiden tuomista eduista.

Kun tiedonkeruu ja tietojen käyttötarkoitukset ubiikkiympäristössä laajenevat ja piiloutuvat, ne antavat moninkertaistuvan edun tiedon hallinnoijille ja hyödyntäjille. Heidän näkökulmastaan vaikutusvalta, toiminnallisuus ja tiedon volyymi kasvaa. Henkilöille, joista tietoa kerätään ja joiden tietoja käytetään, ubiikkiympäristö ei tarjoa samankaltaista läpinäkyvyyttä, vaan läpivalaisee usein heidät yksisuuntaisesti.

Verkkomaailman asymmetria

Lessigin käsitys on, että virtuaalitilan yhteiskuntajärjestys muuttuu kontrollin lisääntymisen kautta sen hallinnoijien, kaupallisen sektorin ja julkishallinnon intressien mukaiseksi (Lessig, 2006). Samalla kansalaisen etujen valvonta olisi jäämässä sivuun. Verkkomaailman kehityskulut tukevat jossain määrin tätä käsitystä.

Verkon hallinta, omistus ja sen palvelujen toiminnallisuudet tuovat asymmetriaa. Verkon valvonta, säätely, toimintaehdot ja välttämättömyydet ovat harvoin käyttäjien käsissä. Lisäksi digitaalisten laitteiden, sisältöjen ja medioiden konvergenssi sekä media- ja tietoteknologiayritysten keskittyminen on ollut ilmeinen kehityssuunta verkkomaailman aikana. Verkon teknologioiden ja sisältöjen omistus ja hallinta keskittyy myös laajentuvien ja yhdentyvien tietovarastojen takia.

Vapauden, avoimuuden ja yhteisöllisyyden varhaisista ideaaleista huolimatta, verkko ei ole demokratian väline, jos siihen ei rakenneta avoimuuden ja vaikuttamisen rakenteita. Sisältötuotannon ja vuorovaikutuksen runsaus eivät takaa sitä, että palveluun osallistujilla olisi vaikutusvaltaa palvelujen tuottamiseen tai niiden taustaorganisaatioiden toimintaan (Lessig, 2006).

Lessig puhuu verkkomaailman asymmetrisyydestä, joka johtuu käyttäjän ja palvelun tarjoajan lähtökohtaisesti erilaisista rooleista. Palveluntarjoaja määrittelee pelisäännöt käyttäjälle. Esimerkkinä hän mainitsee AOL:in, USA:n suurimman teleoperaattorin tarjoamat yhteisölliset palvelut.

> ”…potential for control in this community is unlimited – not in the sense that (AOL) would make life miserable…,but in the sense that it has a regulatory tool that others, in both real space and other cyberspaces, do not.” *(Lessig, 2006)*

Palvelujen käyttäjä on väistämättä toisessa asemassa kuin se, joka omistaa palvelut ja välineet tai säätelee niiden käyttöä. Erot näkyvät esimerkiksi käyttäjien oikeuksissa, toiminnoissa ja palvelun hyödyntämisen laajuudessa. Käyttäjien mahdollisuudet tuottaa, hakea, muokata ja poistaa tietoja tai omistaa ja hallinnoida niitä ovat rajatut, vaikka ne tiedot olisivat itse tuotettuja tai itseä koskevia.

Palvelujen toimintaperiaatteet eivät välttämättä ole käyttäjille selvillä, etenkään taustalla toimivan tiedonkeruun ja sen käyttöjen osalta. Ne voivat tulla esille jälkijunassa tai paljastuksina tekniikkaa tuntevien satunnaisen mielenkiinnon pohjalta. Näin tuli ilmi esimerkiksi Facebook -yhteisöpalvelun toiminto, joka keräsi tietoa käyttäjän nettikäyttäytymisestä jopa palvelun ulkopuolella ja näytti näitä tietoja käyttäjän ”ystäväverkostolle” palvelussa (Vara, 2007, Berteau, 2007).

Asymmetrisyys näkyy myös tiedon ja palvelujen käytön volyymissa. Kun Google kokoaa valtavia tietovarastoja tai tiedonkeruuyritykset yhdistelevät henkilöihin liittyviä tietoja eri lähteistä, eivät tietovarastot ole kenenkään muun käsissä. Sama koskee paikannustietoja. Vaikka käyttäjällä olisi pääsy tietovarastoihin, hänellä on yleensä puutteellinen käsitys kokonaisuudesta: tietovarastojen muodostamisesta, tietojen hallinnasta ja niiden käyttötavoista.

Verkon asymmetria voi ubiikkimaailmassa kertautua. Sen läpinäkyvyys voi jäädä pinnalliseksi, sen vuorovaikutteisuus ei välttämättä takaa vaikutusvaltaa ja sen kokonaisuus voi selvitä vain niille, jotka voivat sen rakenteisiin perehtyä. Sellaisena ubiikkiympäristö olisi melkoisen erilainen kuin se villi ja vapaa verkkomaailma, jossa yhteisöllinen idealismi aikanaan kehittyi.

Ubiikkiyhteiskunnan ongelmat

Haavoittuva kansalainen

”We are who we were.”

- Susanne Lace

Kansalainen on ubiikkiyhteiskunnassa haavoittuvampi. Arjen ja yhteiskunnan elintärkeät toimet ovat ubiikkiympäristössä yhä syvemmin tietojenkäsittelystä ja kansalaisiin liittyvistä tiedoista riippuvaisia. Tiedoilla voi olla myös kansalaisen oikeuksia kaventavia ja yhteiskunnan toimintamalleja merkittävästi muuttavia vaikutuksia.

(Lessig, 2006)

Lace tiivistää ubiikin tietotalouden uhkat kansalaisille seuraaviksi:

- kansalaisen epäoikeudenmukainen kohtelu tietovirtojen ja analyysien pohjalta
- kansalaisella ei ole mahdollisuutta kontrolloida tietovirtoja
- henkilökohtaisen alueen ja toimivallan kaventuminen
- riskiryhmiin luokiteltujen kansalaisten elämänvalintojen vaikeutuminen. *(Lace, 2005)*

Älykkäämmät teknologiat, joilla yhdistellään henkilöhistoriasta koottuja tietoja ja reaaliaikaista tapahtumatietojen virtaa, piirtävät henkilöistä ja ryhmistä uudenlaisia kuvia. Tilaajan intressit ja määritykset voivat vaikuttaa sen tulkintaan, millaisia tuloksia saadaan. Uusilla sosiaalisen erottelun ja segmentoinnin malleilla voi myös syntyä yhteiskuntaan myös uudenlaista epätasapainoa – taloudellisia, sosiaalisia, kulttuurisia ryhmiä, joiden väliset erot vahvistuvat (Lace, 2005).

Tiedonkeruun laajentuessa kansalaisten tietoisuus sen vaikutuksista on jäänyt vähäiseksi. Esimerkiksi Britanniassa vuonna 2004 tehdyssä tutkimuksessa 58 % vastaajista ilmoitti, ettei ymmärrä, miten eri toimijat keräävät ja käyttävät häneen liittyvää tietoa (Lace, 2005).

Ubimaailmassa kansalaisten ymmärrys tiedonkeruusta ja käytöistä on katoamassa horisontista. Heillä ei voi olla käsitystä tietovirroista ja niiden vaikutuksista. Kansalaisilla ei välttämättä ole edes pääsyä itseään koskeviin tietoihin, mahdollisuutta tarkistaa niiden oikeellisuutta ja saada näihin korjauksia – eikä ymmärtää, miten ja kuka tietoja käyttää ja mihin tarkoituksiin.

Kontrollin vaikutusten laajentumista ei myöskään voi havaita, koska tiedonkeruu sulautuu verkossa surffailuun ja asiointiin, eivätkä koottu-

jen tietojen käyttötavat välttämättä käy selville. Tunnistuskäytäntöjen muuttuminen pakollisiksi tai vaihtoehdottomiksi antavat kuitenkin vihjeen siitä, kuinka lähellä loppuaan anonyymiys verkossa ja yksityisyys arkisessa ympäristössä ovat.

Ubiikkimaailma kaventaa kansalaisen henkilökohtaisen alueen ja toimivallan lähes olemattomiin. Samalla se siirtää vallan tiedon kerääjille ja hallinnoijille, joiden toimesta häneen kohdistuu syvenevä tiedollinen läpinäkyvyys. Kansalainen tulee riisutuksi, jos niin halutaan. Ubiikkimaailman käytäntöjen seuraukset voivat olla arvaamattomat.

Ubiteknologia voi väärinkäytettynä olla hyvin riisuvaa. RFID-teknologian yhteydessä on puhuttu ns. “sorting door” -kauhuskenaariosta, jossa RFID-siruja kehossa, korteissa, vaatteissa tai esineissä kantava henkilö saataisiin etäluettavalla laitteella muutamassa sekunnissa “luettua” jokaista päällään olevaa ja mukana kuljetettavaa esinettä myöten. Kaikki, mikä kansalaisella olisi sirutettua, tulisi näin ollen läpinäkyväksi.

Kaikkialle ulottuva läpinäkyvyys ei välttämättä lisää yksilön hyvinvointia, eikä demokraattisen yhteiskunnan toimivuutta. Yksityisen alueen kaventumisen ja jatkuvan tarkkailun kohteena olemisen vaikutuksia ei vielä ole juurikaan tutkittu. On kuitenkin esitetty pelkoja siitä, että laajentuva intiimin alueen kaventaminen saattaa häiritä persoonallisuuden ja identiteetin kehitystä sekä kykyä muodostaa pysyviä ihmissuhteita. Ihmisyyden psykologinen perusta, identiteetti ja kyky kanssakäymiseen, rakentuvat siis yksityisyyden ja henkilökohtaisen koskemattomuuden suojassa. *(Lace, 2005)*

> ”It is a basis for the development of individuality. It protects personal autonomy. It supports healthy functioning by providing needed opportunities to relax, to be one’s self, to emotionally vent, to escape from stresses of daily life, to manage bodily and sexual functions, and to cope with loss, shock and sorrow.”
>
> *(Margulis, 2005)*

Paitsi, että kaventunut yksityisyys murentaa ihmisten psyykkisiä selviytymiskeinoja, sillä on laajoja yhteiskunnallisia vaikutuksia. Valvonnan syvenemisen ennakoidaan myös vahvistavan halua olla erottumatta joukosta, vaan pikemminkin taipua valvojan edellyttämiin kompromisseihin. Se tukahduttaisi kulttuuria ja kaventaisi kansalaisyhteiskunnan toimivuutta.

Tietojen väärinkäyttö tai virheelliset tiedot voivat kaventaa toimintamahdollisuuksia arkielämässä. Palvelujen saatavuudessa, tasossa tai hinnoittelussa ja etuuksissa voi olla merkittäviä eroja eri käyttäjäryhmil-

le. Pelkästään luottoihin ja vakuutuksiin liittyvillä rajoituksilla voi olla merkittäviä vaikutuksia esimerkiksi työhön, asumiseen ja terveydenhoitoon. *(Hall, 2005)*

Tietojen väärinkäytön, virheiden ja puutteiden seuraukset saattavat myös jäädä kansalaisen selvitettäviksi. Tilanne voi edellyttää jopa vuosien selvitystyötä viranomaisten ja luotonvalvojien kanssa. O'Harrow, joka on perehtynyt uusien tiedonkeruuympäristöjen ja yhdistelevän tiedonkeruun ongelmiin, kuvaa useita esimerkkitapauksia. Tietojenkäsittelyn virheistä on voinut tulla kuluttajalle taloudellisia seuraamuksia, "mustalle listalle" tai luottokieltoon joutuminen, maineen tai kunnianloukkauksia, rangaistuksia tai oikeudellisia toimia, joiden selvitys on monimutkaista ja pitkäaikaista. *(O'Harrow, 2005)*

Ubiikkiympäristössä tiedon säilytykselle, analysoinnille ja moninaisille käytöille on yhä tehokkaammat välineet. Tiedon väärinkäytöstä on myös vakavammat seuraukset, jotka voivat tuntua oikeuksien, etuuksien ja palvelujen rajoituksina tai maineeseen tai "hyvään nimeen" liittyvinä menetyksinä.

Laajoja oikeudellisia kysymyksiä

Ubiikkiyhteiskunnan oikeudellisiin kysymyksiin etsitään ratkaisuja kilpajuoksussa teknologian kehityksen kanssa. Kehitys etenee niin nopeasti, että kuilu tarvittavan lainsäädännön ja olemassa olevien käytäntöjen välillä kasvaa. Säätelyvajauksen lisäksi olemassa oleva säätely voi rapautua – niin käy esimerkiksi, jos sen periaatteita on vaikea ymmärtää ja soveltaa käytännössä.

Solmujen avaamista vaikeuttaa se, että ubiteknologian toimintaperiaatteet, vaikutukset ja yhteisvaikutukset ovat monimutkaisia. Ne voivat edellyttää paitsi yksittäisen teknologian tuntemista, myös katsomista sen yhteyksiin ja ubiikkiympäristön kokonaisuuteen. Esimerkiksi syventyvä henkilöön liittyvä tiedonkeruu, tapahtumatietojen yhdistely ja tunniste- ja paikkatiedon hyödyntäminen tarjoavat toiminnallisuutta, jolla voi olla yleisiä ja laaja-alaisia vaikutuksia.

Ubiteknologia ei tuo mukanaan vain erilaisia laitteita ja sovelluksia, vaan se yhdistää laitteita, sovelluksia ja tietovarastoja tavoilla, joista syntyy uudenlaisia toimintaympäristöjä ja toimintaperiaatteita – ja lopulta uudenlainen infrastruktuuri. Vastaava sääntely voi edellyttää myös sen periaatteiden ja asian laajemman viitekehyksen uudelleen arviointia.

Ubiikkimaailma luo uudenlaista järjestystä, joka puuttuu sekä yk-

silön intiimiin alueeseen että yhteiskunnan toimintaperiaatteisiin. Se tunkeutuu kansalaisen henkilökohtaiselle alueelle, hänen ihmissuhteisiinsa, omaisuuteensa ja liikkumiseensa, häntä koskeviin tietoihin ja lopulta myös hänen kehoonsa. Näitä koskettavia periaatteita ovat mm. itsemääräämisoikeus, yksityisyys, anonyymiys, tietosuoja, sananvapaus, kokoontumisvapaus ja yhdistymisvapaus. Kaikki näistä periaatteista tulevat sitä suuremmassa määrin haastetuksi, mitä lähemmäksi arkea ubiteknologia tulee.

Kansalaisten oikeusturvaan liittyvät kysymykset ovat ubiikkiympäristössä uudenlaisessa fyysisessä yhteydessä. Kun aiemmin on esimerkiksi yksityisyyden osalta säädelty näkyvää puuttumista kansalaisen elämään, samat säännöt eivät sovellu ubiikkiympäristöön. Käyttäjä ei välttämättä voi havaita hänen arkeensa puuttumista ja hänen tietojensa väärinkäyttöä.

Virheellinen tieto tai tiedon väärinkäytökset eivät kuitenkaan ole virtuaalitodellisuutta, vaan ne voivat saada aikaan tuntuvaa vahinkoa. Millainen suoja kansalaisella säilyy? Onko itseä koskevista tiedoista oikeus tietää? Onko oikeus korjauttaa virheelliset tiedot? Onko oikeus poistattaa itseä koskevat tietonsa palveluista ja rekistereistä? Poistetaanko tietoja enää ylipäänsä, jos halutaankin hyödyntää sekä reaaliaikaista että koko elämänhistorian ajalta koottuja tietoja, yhdistellä niitä ja luoda niistä profiileja eri tarkoituksiin?

Ympäristöön sulautuva tiedonkeruu ja käyttäjille näkymätön tiedon hyödyntäminen tuo tiedonkeruun kohteille paitsi palveluja, myös lisääntyviä riskejä. Mitä tietoa on oikeus kerätä? Miten tietoa on oikeuskäyttöö, säilyttää, yhdistellä ja jakaa kolmansille osapuolille?

Henkilöiden arviointi voi esimerkiksi kevyen tai epäluotettavan tiedon varassa siirtyä liukkaille jäille. Saako analyysin keinoin piirtää haluamansa kaltaisen kuvan henkilöstä valikoimatta tiedonlähteitä? Millä perusteella ja millaisen tiedon pohjalta kansalaisten oikeuksia, etuuksia ja kelpoisuutta tullaan arvioimaan? Kuka vastaa virheellisistä tiedoista ja niiden aiheuttamista seurauksista? Kuluttajansuojaa ja oikeusturvaa tarvitaan ehkä entistäkin enemmän.

Keskeisiä teemoja ovat myös tekijänoikeudelliset, kilpailuoikeudelliset, immateriaalioikeuksiin, tietokantaoikeuksiin sekä sopimusoikeuteen liittyvät kysymykset (Liikenneministeriö, 2006). Kenellä ovat oikeudet tietoihin, palveluihin ja teknologioihin? Ja millaiset oikeudet? Miten sopimukset tehdään palveluntarjoajan ja käyttäjän välillä? Voivatko ubiympäristössä älykkäät teknologiat tehdä sopimuksen käyttäjän puolesta?

Omistajuuteen, tietojen hallintaan ja hyödyntämiseen kuuluvat myös vastuut. Kuka saa valvoa ja ketä? Palvelujen tuottajilla on esimerkiksi kasvavia intressejä paikkatietoon (kartat, liikenneväylät, rakennukset, kaavat, ilmakuvat). Niiden käyttäjillä voi puolestaan olla hyödyllisiä, haitallisia tai rikollisia syitä seurata kohdehenkilöiden sijaintia ja liikkeitä. Ja jos teknologiat mahdollistavat tunnistamisen, paikantamisen, jatkuvan tiedonkeruun ja seurannan, saako kuka tahansa koota tietoja kenen tahansa sijainnista, liikkeistä, ihmissuhteista ja omaisuudesta?

Kapeneva yksityisyys

Yksityisyys on ubimaailman suurin kansalaisia koskettava ongelma. Suomalaiset ubiteknologian kehittäjät ovat jo havainneet tämän.

> "Oikean tasapainon löytäminen yksityisyyden suojan ja hyödyllisen tietojen jakamisen välillä on yksi ubimaailman kriittisimpiä kysymyksiä." *(Liikenneministeriö, 2006)*

Yksityisyyttä suojaavaa lainsäädäntö on kehittynyt feodaaliajan taitteesta, jolloin orjien ja herrojen välinen raja-aita haluttiin purkaa. Modernien valtioiden muodostuessa ja Ranskan vallankumouksen ideaalien myötävaikutuksella, niiden arvoihin siirtyi henkilökohtainen vapaus – ”masterless man” (Torpey, 2000). Yksityisyys tarkoittaa siis satoja vuosia sitten kansalaisille oikeusvaltioon luotua suojaa, jota pidettiin merkittävänä yhteiskunnallisena saavutuksena.

Yksityisyyden suoja on kuitenkin alkanut kansainvälisesti katsoen heikentyä. Taustalta löytyvät laajentuneen tiedonkeruun, valvontateknologioiden leviämisen, kansainvälisten tiedonvaihtosopimusten ja lainsäädännöllisten muutosten yhteisvaikutukset.

Tiedonkeruu kansalaisista on jatkuvasti kasvanut – erityisesti heidän sijaintiaan, viestintäänsä ja taloudellista tilaansa koskeva tiedonkeruu. Yksityisyys on kaventunut myös valvontateknologioiden kaupallisen menestyksen myötä, minkä vauhdittajia ovat olleet monet kansainväliset tietoteknologiayritykset. *(Privacy international, 2007)*

Viime vuosina parlamentit eri puolilla maailmaa ovat hyväksyneet lainsäädäntöä, jolla on merkittävästi laajennettu viranomaisten otetta kansalaisten yksityiselämään. Perusteluina on käytetty mm. turvallisuutta, siirtolaispolitiikka, sosiaaliturvan väärinkäytöksiä ja hallinnon tehostamista. Samaan suuntainen vaikutus on ollut kansainvälisillä tiedonvaihtoon liittyvillä sopimuksilla. Vaihtosopimusten on usein arvosteltu jopa ohittavan demokraattisia ja oikeudellisia prosesseja.

(Privacy international, 2007).

Suomessa yksityisyyttä suojaavia nykyisiä säädöksiä ovat mm. sananvapaus, kotirauha sekä säännökset esitutkinnasta (Liikenneministeriö, 2006). Lainsäädäntö on kuitenkin syntynyt ympäristössä, jossa yksityisyyteen tunkeutumiseen on kuulunut fyysinen läsnäolo tai yksittäisten teknisten apuvälineiden käyttö (esim. kamera). Konflikti ja sen aiheuttaja ovat olleet selviä. Ubiikkiympäristössä tilanne tulee olemaan toinen. Kohdehenkilölle ei välttämättä tule olemaan selvää, kuka kerää, varastoi, siirtää ja käyttää hänen tietojaan ja mihin tarkoituksiin.

Kompromissiratkaisuksi ubiikkiteknologian kehittäjät ovat ehdottaneet, että "yksityisyydestä tulee dynaaminen prosessi, jolla neuvotellaan ja hallitaan oman tilan ja julkisuuden teknisiä ja sosiaalisia reunaehtoja" (Liikenneministeriö, 2006). Menettelyllä rajattaisiin tunnistuksen, paikannuksen ja valvonnan käyttöjä sellaisiin yhteyksiin, joissa eri osapuolet sopivat keskenään tiedon luovutuksesta. Kohdehenkilö voisi näin jossain määrin neuvotella oman yksityisyytensä rajoista.

Käsityksessä on omat ongelmansa. Se, mihin tietojen käyttökiellolla tai sallimisella voi puuttua, on käyttäjälle keskeinen asia. Hänen pitäisi tietää, mitä tietoja kerätään, miten palvelun tietoja käytetään ja päätyvätkö ne kolmansien osapuolien käsiin tiedonsiirron, vaihdon, yhteiskäytön tai myynnin perusteella? Sitä voi olla vaikea ymmärtää tai se voi selvitä vasta myöhemmin. Esimerkiksi Facebook-verkkoyhteisöön sisältynyt piilotettu käyttäjien seuranta ja tietojen lähetys "ystäväverkostolle" on kuvaava käytäntö – käyttäjille näkymätön toiminnallisuus selvisi vasta, kun tekniikkaa tunteva käyttäjä kävi lukemaan, mitä koodi todella tekee (Berteau, 2008).

Katoava tietosuoja

Tietosuojasäännökset tulivat laajemmin käyttöön 1980-luvulla laajentuvan automaation ja tiedonkeruun myötä. Säännöksissä määritellään yleensä, mitä henkilöön liittyvää tietoa voidaan kerätä ja käyttää, millaisia laatuvaatimuksia tiedoille asetetaan, mikä on tietojen säilytysaika, mitä kansalainen saa tietää häntä koskevista tiedoista ja miltä osin hän voi vaatia muutoksia tai poistoja tietoihin. *(Perri 6, 2005)*

Ubiikkiympäristön tehostuva ja ympäristöön kätkeytyvä tiedonhallinta laajentaa jo sinänsä tietosuojan tarvetta. Se tuo myös uudenlaisia riskejä, kuten

- salaisten tietovarastojen rakentumisen, joista käyttäjät eivät ole tietoisia
- salassa tehtävän tietojenkäsittelyn, josta tietojen kohdehenkilö ei voi tietää

- luvattoman tietojen käytön, jossa käsitellään tietosuojan alaista tietoa
- laittoman tietojenkäsittelyn, joka on selkeästi kansallisten tai kansainvälisten säädösten vastaista
- puutteellisten, virheellisten tai päivittämättömien tietojen tarjonnan
- puutteellisen valituskäytännön, jossa palveluntarjoaja ei vastaa tietojen muutospyyntöihin
- tiedon käsittelyn tietosuojasäädöksien tai lainsäädännön ulottumattomissa (esim. tiedot siirretään käsiteltäväksi toiseen ympäristöön tai maahan, jossa säädöksiä ei tarvitse noudattaa)
- tiedonkäsittelijä ei ota vastuuta tiedon laadusta ja ajantasaisuudesta *(Borking, 2005)*

Ratkaisut näihin ovat tietosuojakysymyksiä. Paradoksaalista kuitenkin on, että henkilöä koskevan tiedonkeruun alan laajentuessa ja tiedonkäsittelyn tehostuessa, näyttäisi paineita olevan pikemminkin tietosuojan purkamiselle (Liikenneministeriö, 2006).

Tietosuojan merkitys on alkanut hämärtyä myös käyttäjien näkökulmasta. Käyttäjille puhutaan nykyisellään yhä useammin tietoturvasta tavalla, joka on omiaan antamaan käsityksen, että tunnistettu verkkoon kirjautuminen takaisi verkkoasioinnille suojan. Tietoturvalla ei kuitenkaan puututa tietojenkäsittelyn luonteeseen palvelussa, eikä esimerkiksi vähennetä yhtäkään Borkingin edellä mainitsemista riskeistä. Se, mitä palveluntarjoajan tietojenkäsittelyssä tapahtuu ja mihin tietoja käytetään, on kansalaiselle vähintäänkin yhtä tärkeä kysymys kuin tietoturva.

Tiedon väärinkäyttö

Kun jo nykyisessä Internet-ympäristössä on nähty teknologioiden väärinkäyttöä, tietojen kalastamista, roskapostia ja hakkerointia, on todennäköistä, että myös tulevissa kehitysvaiheissa havaitaan nopeasti erilaiset väärinkäytön mahdollisuudet. Niihin kuuluvat verkkorikollisuus yhtä hyvin kuin vähäisemmät tietoturvaan liittyvät ongelmat.

> ”Given the almost unlimited potential of everyware to facilitate the collection of all sorts of information, the extreme subtlety with which ubiquitous systems can be deployed, and the notable propensity of certain parties – corporate, governmental – to indulge in overreaching information gathering activities if once granted

> the technical wherewithal, I would be very surprised if we didn't see some highly abusive uses of this technology over the next few years. *(Greenfield, 2006)*

Väärinkäytökset ja varkaudet verkkoympäristössä eivät ole satunnaisia, vaan niistä on jo tullut yleisiä ja laaja-alaisia ongelmia. Näistä suurimpia ongelmia aiheuttavat identiteetti- ja tietovarkaudet. Yleistä on myös luottamuksellisten tietojen väärinkäyttö organisaatioiden sisällä.

Väärinkäytösten kohteina voivat yksittäiset kansalaiset, yhteisöt tai yhteiskunnan toiminta laajemmin. Esimerkiksi tietovarkaudet ovat kohdistuneet usein suureen joukkoon verkon palvelujen käyttäjiä.

Identiteettivarkaudet ja verkkohuijaukset ovat USA:ssa levinneet epidemian tavoin. Gartner Inc.:n mukaan USA:n identiteettivarkaudet kohdistuivat 7 miljoonaan henkilöön vuonna 2003 ja niiden määrä on myöhemmin noussut yli kaksinkertaiseksi (O'Harrow). Vuoden 2007 aikana on verkossa huijatun rahan määrä Yhdysvalloissa arvioitu 2,2 miljardiksi dollariksi ja huijausten uhrien määrän arvioidaan nousevan 3,6 miljoonaan (Linnake, 2007).

Tietovarkaudet, joissa henkilöihin liittyviä tietoja myydään suurina erinä, ovat myös merkittävää vahinkoa aiheuttava väärinkäytösten laji. Hiljattain uutisoitiin tietokannan ylläpitäjän myyneen 8,5 miljoonaa Fidelity National Servicen asiakastietuetta tietopalveluyritykselle (Mannila, 2007). Edellisenä vuonna intialaiset Call Centerin työntekijät kaupittelivat tuhansien brittien luottokorttitietoja (Kirves, 2006).

Tiedot voivat hävitä muillakin tavoilla. Harris Interactiven 2006 tekemän tutkimuksen mukaan yksi viidestä amerikkalaisesta oli saanut ilmoituksen yritykseltä tai julkishallinnon organisaatiolta siitä, että hänen liittyviä tietoja oli kadonnut, varastettu tai väärinkäytetty (Washington Post, 2000). Esimerkiksi brittiviranomaiset kadottivat hiljattain 25 miljoonan henkilön lapsilisien maksamiseen liittyvät tiedot (CNN Europe, 2007).

Viranomaisten tekemät virheet tai väärinkäytökset eivät ole tavattomia muissakaan muodoissa. Amerikkalaiselle Amnesty International –aktivistille tuli yllätyksenä, että Denverin poliisi oli luokitellut hänet ja joukon muita kansalaisaktivisteja viranomaisen tietokantoihin "rikolliseksi ääriaineksiksi" ("criminal extremist") – joukossa oli mukana mm. köyhien intiaanien parissa työskentelevä nunna. Virheiden seuraukset olisivat saattaneet olla vakavia kyseisille henkilöille, jos järjestelmän tiedot olisivat tulleet vastaan esimerkiksi maan rajalla matkalle lähtiessä. *(O'Harrow, 2005)*

Tiedonlouhinnan tai älykkäiden ohjelmien päättelyperiaatteet eivät välttämättä ole vedenpitäviä. Esimerkiksi rikosepäillyksi voi leimautua, jos henkilön sattumanvaraiset suhteet ja yhteydet on tulkittu väärin. WTC:n terrori-iskun jälkimainingeissa pidätettiin mies, joka oli lunastanut ajokorttinsa samassa viranomaisen toimistossa muutama minuutti sen jälkeen, kun rikollinen oli hakenut oman korttinsa. Koska molemmilla miehillä oli arabiankielinen sukunimi, tehtiin virhepäätelmä henkilöllisyydestä. (*Klosek, 2007)*

Tiedon hallinnoijien kynnys tietojen väärinkäyttöön on näyttänyt olevan matalalla. Jos välineet ovat antaneet tilaisuuden, on löytynyt myös varkaita. Cyber-Ark-Softwaren tekemän tutkimuksen mukaan joka kolmas IT-alan työntekijä on myöntänyt tutkimuksessa väärinkäyttäneensä käyttöoikeuksiaan tietojärjestelmiin ja katsoneensa luottamuksellisia tietoja. Esimerkiksi työtovereiden tiedostoja ja sähköposteja on luettu tai katsottu henkilöstöhallinnon tietoja.

(Poropudas, 2007a)

Tiedot saattavat tulla tulkituiksi tavoilla, joka ei tee kohdehenkilölle oikeutta – puutteellisesti tai yhteyksistään irrallaan. Tulkintavirheet eivät välttämättä tule koskaan julki. Jos henkilö olisi oikeutettu palveluun tai kuulumaan kohderyhmään, mutta on jäänyt sen ulkopuolelle, ei hän ehkä koskaan tule tietämään menetetystä tilaisuudestaan.

Tarjolla olevien taustatietojen käyttö on myös tullut entistä epämääräisemmäksi. Elämänhistorian ongelmien, ulkopuolisten määrittämien poikkeamien tai rajojen ylityksien vaikutukset voivat tulla arvaamattomiksi ja kohtuuttoman pitkäikäisiksi. Verkkotiedon yhä pidempiaikaisesta säilytyksestä ja sen väärinkäytön mahdollisuuksista, jotka ovat vaikuttaneet esimerkiksi henkilöiden myöhempiin elämänvalintoihin, työhön ja maineeseen, on lukuisia esimerkkejä (Goodin, 2007). Amerikkalaiset työnantajat ovat jopa jälkikäteen irtisanoneet ihmisiä, joiden taustasta on seurantaselvitysten perusteella löytynyt pieniä rikkeitä (esim. 60 $ katteettoman sekin kirjoittaminen, joka vastaa tilin ylitystä).

(O'Harrow, 2005)

Oma lukunsa on viihteellinen tai yksityishenkilönä tuotettu verkkotieto, jonka luotettavuudesta, autenttisuudesta ja motiiveista ei ole takeita. Oireita epämääräisten tiedonlähteiden huomioimisessa työntekijöiden arviointiin on myös Suomessa. Viranomaiset ja työnantajat näyttävät jo nyt reagoivan kevyeen verkkotietoon henkilöiden arvioinnissa tai rekrytoinnissa (Poropudas, 2007b, Aktuellt, 2007).

Kansalaisen kannalta, joka ubiikkiyhteiskunnassa luovuttaisi yhä enemmän tietojaan yritysten ja julkishallinnon käsiin, eivät väärinkäytösten näkymät enteile hyvää. Tietovarastojen laajentuessa riski henkilön tietojen joutumisesta väärin käsiin laajentuu merkittävästi. Tiedoilla voidaan myös aiheuttaa nopeammin ja tuntuvampaa vahinkoa.

Uudet välineet ja julkinen verkkotieto näyttävät myös tuottavan uudenlaisia käytäntöjä, joissa henkilöiden arviointitavat ovat muuttuneet jyrkemmiksi ja hyödynnettävien tietojen oikeellisuus ei ole taattua. Se on kansalaisen kannalta oikeusturvaongelma.

Demokratiavaje ja sen uhat

Ubiikkiyhteiskunnan eteneminen näyttää aiempia yhteiskunnallisia siirtymävaiheita riskialttiimmalta. Tasapaino hyötyjen, haittojen ja erilaisten intressien välillä on herkempi. Reaaliaikainen tiedonkeruu, laajat tietovarastot ja tehokkaat teknologiat antavat ennen näkemättömät hallinnan ja valvonnan välineet. Niiden mahdollistama laajentunut ja tarkentunut maailman hallinnan ala tekee ubiikkiympäristöstä myös otollisen kohteen valtataistelulle ja konflikteille.

Konfliktiherkkyys

Erilaisten valtaintressien voimistuminen ja konfliktien kärjistyminen on mahdollista, kun ubiteknologialla voidaan hallinnan ja valvonnan mahdollisuuksia laajentaa kaikkialle. Valtaa haluavia intressiryhmiä voi löytyä esimerkiksi poliittisten, taloudellisten, uskonnollisten tai rikollisten tahojen takaa. Ubiikkiteknologian mahdollisuuksien joutuminen vääriin käsiin olisi suunnattoman ongelmallista yhteiskunnalle, kansanryhmille tai yksittäisille kansalaisille.

Ongelmia voi syntyä myös poliittisen järjestelmän tasapainon menetyksestä ja kansainvälisistä konflikteista. Kansainväliset sopimukset ja sitoumukset voivat puolestaan muuttaa esimerkiksi tietovarastojen käyttötapoja ja välittää kansalaisten tietoja käyttöihin, joita ei aiemmin ajateltukaan. Entäpä sitten, jos älykkäiden tiedonhallinnan teknologioilla käydäänkin seulomaan ja seuraamaan tiettyjä kansalaisryhmiä tai vähemmistöjä esimerkiksi poliittisista tai uskonnollisista syistä tai kansainvälisen turvallisuuden tarpeista käsin?

Vallan siirtyminen ja kätkeytyminen

Toimivallan huomaamaton siirtyminen julkiselta sektorilta yksityisen sektorin käsiin on jo havaittu ongelma. Esimerkiksi tiedonkeruuyritys-

ten ja julkishallinnon laajamittaisen yhteistoiminnan on katsottu muuttaneen amerikkalaisen yhteiskunnan tasapainoa ja siirtäneen toimivaltaa yrityksille (O'Harrow, 2005). Vielä ongelmallisempaa on, kun tietoja, joiden luotettavuutta ei voida taata, hyödynnetään lisääntyvään valvontaan (Andrejevic, 2007). Amerikkalaisten tiedonkeruuyritysten toimintaa on arvosteltu juuri näistä syistä.

> ”By outsourcing the collection of records, the government doesn't have to ensure the data is accurate, or have any provisions to correct it in the same way it would under the Privacy Act.”
>
> *(O'Harrow, 2005)*

Ubiikkimaailmassa tietojenkäsittelyprosessit ovat kätketympiä, jolloin pahimmassa tapauksessa voi tapahtua tietoista huomaamatonta vallansiirtoa halutuille ryhmille. Esimerkiksi massiivinen ja huomaamaton tiedonkeruu ilman tiedon käyttöihin ja tietojenkäsittelyyn liittyvää kontrollia avaisi houkuttelevan tien kansalaisen oikeuksien vastaisille toimille ja vallansiirroille.

Euroopan tietosuojavaltuutetut ovat arvostelleet jo teletunnistetietojen tallennusta siitä, että järjestelmä mahdollistaa salaisen tunnistetietoihin perustuvan valvonnan kehittymisen (Aarnio, 2005). Suomessa teletunnistetietojen keräämiseen on myös kohdistettu kritiikkiä. Säilytysvelvoitteiden ohella yrityksille ei ole näyttänyt tulevan tiedonkäsittelyyn liittyviä vastuita. Miten taataan, että tietoja käytetään oikeisiin tarkoituksiin, tietoihin eivät pääse ulkopuoliset ja että tiedot ovat oikeita? Miten käy sitä paitsi teleyritysten omaan toimintaan liittyvän valvonnan, kun tiedot ovat heidän omassa hallinnassaan? *(Kasvi, 2005)*

USA:ssa on näytetty mallia jopa kehityksen päinvastaisesta suunnasta - tietojenkäsittelijöiden vastuiden purkamisesta. Teleyrityksiä on lähdetty suojaamaan väliaikaisella lainsäädännöllä, joka antaa yrityksille syytesuojan (legal immunity) mahdollisten oikeussyytteiden varalta – eli vahvistaa, etteivät yritykset joudu vastuuseen tietojen käytöistään. Lainsäädännön mahdollinen jatkaminen on kuitenkin saanut aikaan näkyvän julkisen keskustelun ja vastustuksen (esim. Singel, 2008, Fredrickson, 2008).

Uhat eivät ole kaukaa haettuja. Julkishallinnossa käytetään yhä enemmän ulkoistamista ja yksityisen sektorin palveluja, joihin tietokantojen, rekisterien ja tietovarastojen hallinta voivat myös kuulua. Valtion ja kuntien IT-strategiat kannustavat viranomaisia palvelujen keskittämiseen ja ulkoistamiseen (Valtiovarainministeriö, 2006, Valtiovarainministeriö, 2007b). Kun tietovarastojen keskittäminen ja yhteiskäyttö helpottavat

tietoihin pääsyä, ne myös lisäävät niiden väärinkäytön mahdollisuuksia. Kun tietojen perusteella tehdään oleellisia kansalaisten elämään liittyviä päätöksiä, pitäisi huolehtia, että tietojenkäsittelyä valvotaan ja että tietosuoja voidaan taata.

Kansainvälinen tietojen vaihto

Omat ongelmansa tuottavat kansainväliset tietojen siirrot ja tietojen vaihto. On esitetty yleisemmin pelkoja siitä, että kansalaisen oikeusturvaan liittyviä säädöksiä kierretään siirtämällä toiminta kolmansiin maihin, joiden lainsäädäntö on väljempi (Nieminen, 2007). Sama huoli voi koskea tietojenkäsittelyä.

Kansainväliset yritykset voivat säilyttää julkishallinnon keräämää tietoa kansalaisista missä maassa tahansa. Maan rajojen ulkopuolella tietoja eivät välttämättä koske säädökset, jotka suojaisivat niitä kotimaassa. Kansalaisia koskevien tietovarastojen kontrolli saattaisi ulkoistamisen tai yksityistämisen myötä myös kadota demokraattisen valvonnan piiristä.

Kyse ei välttämättä ole vain kansalaisen oikeusturvasta, vaan myös laajemmin yhteiskunnan edusta. Esimerkiksi Ruotsissa turvallisuuspoliisi (SÄPO) on varoittanut teletunnistustietojen keruuta koskevan lainsäädännön käsittelyn yhteydessä, että tietojen säilytys maan ulkopuolella ja mahdolliset muut käytöt näissä maissa voivat tuoda mukanaan ennakoimattomia vaikutuksia, jotka voivat kääntyä valtion etua vastaan (SOU 2007).

> ”Huruvida uppgifter som finns i ett lager i ett annat land kan få spridning utöver vad som följer av svensk rätt beror på den rättsliga regleringen i landet där lagret finns. Det finns med andra ord inte någon garanti för att uppgifter som lagras i ett annat land inte används för andra ändamål än de som den svenska lagstiftningen medger.” (SOU 2007:76)

Samat ongelmat voivat tulla vastaan myös viranomaisten välisessä kansainvälisessä tietojen vaihdossa ja yhteiskäytössä. Sopimuksien sisältö ei ensinnäkään välttämättä rajaudu siihen, mikä näyttäisi olevan sen päätarkoitus. Esimerkiksi Prümin sopimus, josta on ensi sijassa puhuttu terrorismin torjuntaan tarkoitettuna tiedonvaihtosopimuksena, ei rajaa tietojen käyttöä vakavien rikosten selvittämiseen ja rikollisten etsintään. DNA- ja sormenjälkitietojen luovuttamista voidaan tehdä riippumatta rikoksen tyypistä ja kansalaisen roolista rikostutkinnassa. Hän voi olla epäilty, asianomistaja tai sivullinen. *(Kasvi, 2006)*

Ruotsissa on esitetty myös huoli siitä, että ulkomaisille osapuolille

voitu on antaa sopimuksessa laajemmat oikeudet käyttää tietoja kuin kotimaisille viranomaisille, jotka tarvitsevat tietoihin oikeuden päätöksen, kun taas ulkomaiset osapuolet eivät tätä tarvitse (DS 2007:47).

Oma ongelmakenttänsä on vaihtosopimusten perusteella annettujen tietojen mahdollinen väärinkäyttö ”turvattomissa” maissa (Evans, 2005, 120). Jos kansalaisten tiedot pääsevät maan rajojen ulkopuolella vääriin käsiin esimerkiksi maan epävakaiden olojen tai korruptoituneiden viranomaisten takia, ne tuovat kansalaisille oikeusturvaongelmia. Cybercrime-sopimuksen tietojenluovutusvelvollisuuden perusteella voivat esimerkiksi Albania ja Venäjä saada teletunnistetietoja käyttöönsä (EFFI, 2007).

Demokraattisen järjestelmän ongelmat

Teknologian väärinkäyttö kansalaisyhteiskunnan vastaisilla tavoilla voi johtua myös demokraattisen järjestelmän ongelmista. Pelkästään verkkosensuurin otteen laajentumisesta on huolestuttavia merkkejä viime vuosilta eri maista. Viiden vuoden sisällä verkkosensuurin käytännöt ovat levinneet muutamasta valtiosta 12 valtioon (Boyd, 2007).

Kiina on saanut ehkä eniten kuuluisuutta nettisensuurinsa takia. On valitettavan kuvaavaa, että Microsoft poistatti kiinalaisista MSN Spaces blogeista mahdollisuuden käyttää sanaa ”demokratia” (Andrejevic, 2007). Sisällöllisten rajausten lisäksi kiinalaiset ovat halunneet kehitellä välineitä, joilla seurattaisiin verkkoyhteisöjä ja niiden ei-toivottuja muotoja.

> ”…Zhao Jing identified in published news accounts the nature of the line he´d crossed: ‘If you talk every day online and criticise the government, they don’t care…Because it’s just talk. But if you organise – even if it’s just three or four people – that’s what they crack down on. It’s not speech: it’s organising.’ Microsoft, with an eye to the lucrative potential of the Chinese market, helped take the activism out if interactivity…”
>
> *(Andrejevic, 2007)*

Amerikkalaisten ja kiinalaisten teknologiayritysten yhteistyö on johtanut moniin valvontaa edelleen syventäviin hankkeisiin. Vuonna 2007 Schenzenissä Kiinassa asennettiin 20 000 valvontakameraa kaduille. Kameravalvonta on yhdistetty kasvontunnistusta hyödyntävään kuvaanalyysiin, jonka perusteella kaduilta voidaan tunnistaa halutut henkilöt. Kiinassa käyttöön on tulossa myös RFID-pohjainen id-kortti, jonka muistiin tallennetaan poikkeuksellisen laajat tiedot kansalaisista, kuten

työhistoriaan, koulutukseen, rotuun, uskontoon, rikosrekisteriin ja terveyteen liittyviä tietoja. *(Bradsher, 2007)*

Demokraattisten maiden huonoin tilanne on USA:ssa, jossa valvontaan liittyvät hankkeet ovat jatkuvasti lisääntyneet (Privacy International, 2007). Tietojärjestelmiä, joissa valvontakameroita, kasvojen tunnistusta ja sosiaalisten verkostojen analyysia yhdistellään, kehitellään myös USA:ssa myös viranomaisten käsiin (Legge, 2008). Yhä tarkempi valvonta on eri muodoissaan laajentumassa julkisiin laitoksiin ja työpaikoille. Kouluissa kokeillaan esimerkiksi valvontakameroihin yhdistettyä kasvojentunnistusta erottelemaan tuntemattomat kasvot käytäviltä ja tiloista (Bottorff, 2007).

WTC:n terrori-iskun jälkeen valvontateknologia kehittynyt, tiedonkeruu laajentunut ja useampien lainsäädännöllisten muutoksien tuella valvontaa on jatkuvasti laajennettu. Lisäksi valvonnan luonne näyttäisi laajentuvan rikollisten seurannasta yhteiskunnallisesti aktiivisiin kansalaisiin ja koko väestöön. Aiemmin mainittu Denverin poliisin tiedonkeruu ja kansalaisten väärin luokittelu paljastaa osan ongelmasta. Kohtalaisen rauhanomaista kansalaisaktivismia harrastaneiden nimet olivat koottuina paikallisen poliisin tietokantoihin. On demokratian kannalta oireellista, jos kansalaisaktivismiin pitää viranomaiskeinoin puuttua tällä tavoin. *(O'Harrow, 2005)*

Valvonnan ulottaminen verkkoon, kansalaisten ihmissuhdeverkostoihin ja julkisille paikoille sekä sen kohdistaminen yhteiskunnallisesti aktiivisiin kansalaisiin tai koko väestöön ovat käytäntöinä laajentumassa. Ne rikkovat oikeusvaltioiden perustuslakeja ja kansalaisen perusoikeuksia, joihin kuuluvat yksityisyys, sananvapaus, mielipiteen vapaus, yhdistymisvapaus ja kokoontumisvapaus. Nämä perusoikeudet tulevat jatkossakin haastetuiksi, jos valvonnan teknologioiden käyttö ja niiden yhdistely laajentuviin tietovarastoihin ja tunnistuskäytäntöihin jatkaa leviämistään, eikä niille aseteta rajoja.

Julkishallinnon toimintaperiaatteiden muutos

Uudet tiedonhallinnan mallit voivat myös muuttaa julkishallinnon toimintaperiaatteita. Britanniassa tiedonlouhintaa on hyödynnetty jo vuosia. Käytännöt ovat niveltyneet poliittisiin ohjelmiin, joilla pyritään esimerkiksi terveydenhuollon, opetusalan ja työllisyyden alueelliseen ja rakenteelliseen kehittämiseen.

Menetelmiä hyödynnetään esimerkiksi aluesuunnitteluun sekä julkishallinnon palvelujen tehostamiseen ja kohdentamiseen. Profilointia ja

henkilötietojen analysointia käytetään esimerkiksi rikosten selvittämiseen, riskien arviointiin lastensuojelun ja mielenterveyden palveluissa, veropetosten ja sosiaalietuuksien väärinkäytön tutkintaan sekä terveydenhuollon palvelujen kohdentamiseen.

(Lace, 2005, Perri 6, 2005)

Kehittämistoimiin sisältyy tietojen vaihtoa (data sharing) ja yhdistelyä (data matching) sekä riskiryhmien analysointia (risk assesment, social sorting), joilla on pyritty jäljittämään viranomaisten kannalta ongelmalliset ryhmät ja yhteisöt.

> ”This plan places much emphasis on inter-agency data sharing, in order to identify communities, minorities and groups of individuals ‘requiring tailored and targeted interventions’ that are to be both intelligence-led and supported by multi-agency working”
>
> *(Bellamy, 2005)*

Lace näkee keskeisenä ongelmana tiedonhallinnan teknologioiden edellyttämän kohderyhmien määrittelyn, jonka hän näkee antavan uudenlaisia piilossa olevia vallankäytön välineitä viranomaisille (Lace, 2005). Uudenlainen kansalaisryhmien erottelu ja palvelujen tehokkaampi kohdentaminen saattavat vahvistaa kansalaisryhmien välisiä rajoja ja eroja ja syventää epätasa-arvoa. Kansalaisryhmien erottelu (social sorting) voi muodostaa uusia ongelmia, kuten kohderyhmään valinta tai sen ulkopuolelle jääminen, etuuksien saannin ongelmat, oikeuksien riisto ja syrjintä (Raab 2005)

Ubimaailman tiedonhallinnan teknologiat haastavat laajemmin käsitykset siitä, mitä on sopiva käyttäytyminen, identiteetti, kansalaisuus, työ ja yhteiskunta (Raab, 2005). Ne muuttavat nykyisiä käsityksiä ja tuottavat uudenlaisia rajoja.

Ubiikkiympäristössä on nykyistä ongelmallisempaa, jos salaisten erotteluun liittyvät periaatteet ovat tuntemattomia tai puutteellisia ja taustalla toimiva informaatioprosessi on piilossa kansalaisilta. Pahimmillaan kansalaisryhmien erottelusta voisi tullakin teknologia-avusteista syrjintää tai demokraattisten rakenteiden puuttuessa jopa vainoa. Julkishallinnon toimintaperiaatteilta ubiikkiympäristössä tulisikin edellyttää läpinäkyvyyttä.

Oleellista on myös, millaisia pakkoja ja toimintamalleja ubiikkimaailmaan luodaan. Onko kansalaisen elettävä vuorokauden ympäri siten, että hän on paikannettavissa ja hän liikkuu ja asioi tunnistettavasti? Tuoko fyysisen ja verkkoasioinnin yhdentyminen myös vaihtoehdottomuuden ja elämän yhden kortin varassa?

Greenfield ennakoi viisaasti, että vain vaihtoehtojen säilyminen on demokratiaa. Ubimaailman tärkeimpiä vaihtoehtoja on mahdollisuus

hallita omassa käytössä olevia laitteita, sulkea laite tai irtisanoa sopimus palvelusta. Jos vaihtoehdot lakkaavat, sulkeutuvat demokraattisen yhteiskunnan ovet kolkosti perässämme.

> ”We must see that everyware serves us, and when it does not, we must be afforded the ability to shut it down. Even in the unlikely event that every detail of its implementation is handled perfectly and in a manner consistent with our highest ambitions, a paradise without the choice is no paradise at all.”
>
> *(Greenfield, 2006)*

Läpinäkyvä kansalainen

Miten kansalaisen ääni kuuluu ubimaailmassa?

”Connecto ergo sum”

- Björneborn, 1998

Kansalaisten vaikutusalue verkossa näyttäisi laajentuneen samalla, kun verkkoyhteydet ovat levinneet käyttäjille ja verkon vuorovaikutteisuus on lisääntynyt ja palvelut ovat monipuolistuneet. Jo Internet-kehityksen alkuvaiheissa, fyysisten ja sosiaalisten verkostojen katsottiin tulevan niin merkityksellisiksi, että niistä muodostuu uudenlaisia yhteiskunnan perusyksikköjä (Castells, 1996). Verkkoyhteisöistä on tullutkin perheiden, organisaatioiden ja paikallisten yhteisöjen rajat ylittäviä, usein jopa kansainvälisiä virtuaaliheimoja, joiden vaikutusvallan ennakoidaan jatkossa kasvavan yhteiskunnassa (Mannermaa, 2007).

Yhteisölliset tai Web 2.0 -palvelut, joissa käyttäjät ovat tulleet merkitykselliseksi osaksi kaupallisia ja ei-kaupallisia palveluja, ovat esimerkkejä laaja-alaisista vaikuttamisen kanavista verkossa. Palveluissa ei enää tarjota vain valmiita sisältöjä, vaan niissä on mahdollista keskustella, verkostoitua ja tuottaa sisältöjä. Tunnetuimmat yhteisölliset palvelut, kuten YouTube, FaceBook, MySpace ja Amazon.com antavat käyttäjille jakelukanavan, keskusteluyhteyden ja viestinnän ja verkostoitumisen välineen niiden asioiden ympärille, joista he ovat kiinnostuneita. Samankaltainen vaikutus on blogeilla ja keskusteluryhmillä.

Verkossa vaikuttaminen, jos sitä tarkastellaan vetovoimana käyttäjiin, ei kuitenkaan ole yksiselitteinen ilmiö. Verkkoa voi kuvata yhteyksien ja solmukohtien jatkuvasti uudelleen muotoutuvana verkostona, jota sen käyttäjät jatkuvasti yhdessä kutovat (”collaborative weaving”). Sen solmuista tai palveluista syntyy pienempiä tai suurempia tähtiä riippuen siitä, miten suuren joukon käyttäjiä ne vetävät. Käyttäjien äänet eivät

jakaudu tasaisesti, vaan niistä rakentuu erilaisia sosiaalisia verkostoja (”small world -phenomena”). *(Björneborn, 2004)*

Keskeinen media, satunnainen paikallaolo tai hyvin valittu ajoitus ja sensaatiomainen sisältö ovat verkossa merkitseviä, jos viestillään haluaa vaikuttaa. Verkkomaailman vetovoimaisimmat tähdet sykkivät edelleenkin medioiden ja erilaisten kansainvälisten haku- ja yhteisöpalvelujen ympärillä – Google, Yahoo, CNN, BBC, YouTube ovat käyttäjämääriltään vetovoimaisimpien palvelujen joukossa. Bloggaajien kiinnostus näyttäisi myös kytkeytyvän medioiden keskeisesti esille nostamiin sisältöihin (Thelwall, 2007, mm. BBC, CNN).

Sopivissa tilanteissa viesti voi kuitenkin saada arvaamattomat mittasuhteet. Petteri Järvinen puhuu osuvasti ”sattumajournalismista”, jossa varomattomat sanat verkossa ovat saaneet liikkeelle lumipalloefektin. Vaalitilaisuudessa ollut valpas vastakkaisen puolueen edustaja oli poiminut poliitikon huulilta lipsahtaman sanan, joka välittyi edelleen lehteen negatiivisena tulkintana. Aiheen ympärille rakennetun videon levitys verkossa johti lopulta poliitikon häviöön vaaleissa. *(Järvinen, 2007)*

Voitaisiin puhua myös sensaatiovaikutuksesta, jota verkossa leviävät kansalaisadressit hyvin kuvaavat (http://www.adressit.com/). Lähinnä mediasta nousseet teemat ovat kanavoituneet myönteiseksi tai vastustavaksi reaktioksi, joista onnistuneimmille on saatu nopeasti kerättyä kymmeniä tuhansia kannattajia. Yhteiskunnalliset teemat, sensaatio ja viihde sekoittuvat adressien sisällöissä.

Yhteisöllisten tai Web 2.0 palvelujen on katsottu vaikuttaneen käänteentekevällä tavalla verkon palveluihin ja niihin liittyvään liiketoimintaan. Palvelujen kehitystä ja teknologioiden tuottajia ohjailevat yhä enemmän käyttäjien liikkeet ja heidän toimintansa. Yhteisöllisillä palveluilla on myös ollut kiistämättömästi vaikutuksia päätöksentekoon, medioihin ja näiden luomiin pelisääntöihin. Ne ovat tuoneet asiantuntijoiden rinnalle keskustelijoiksi ja vaikuttajiksi tietystä aiheesta kiinnostuneet harrastajat ja tavalliset kansalaiset – heidän ääntään kuuntelevat kiinnostuneemmin niin valtamediat kuin yritykset.

Eri asia on, miten tai millaisiin asioihin puhe verkossa vaikuttaa. Onko kyse medioiden kysymyksen asetteluun vastaamisesta, kansalaisliikkeestä vai havaintoihin perustuvista näkemyksistä? Saako sähköposti kansanedustajalle, kirjoitus tunnetussa mediassa vai 30 000 nimeä adressissa päättäjät mukaan keskusteluun? Valikoivatko päätöksentekijät, mediat ja yritykset haluamansa viestit tukemaan tarkoituksiaan vai saako esitetty käsitys heidät pohtimaan teemaa uudesta näkökulmasta?

Tiedonkeruun ja analysoinnin käytännöt tekevät toisaalta myös verkkoyhteisöistä kohderyhmiä, joissa käsiteltäviä aiheita ja verkostoitumista voidaan laajalti seurata, olivatpa tarkoitukset kaupallisia tai poliittisia (Andrejevic, 2007). Tiedon analysoinnin välineet antavat jo nykyisellään mahdollisuuden eritellä esimerkiksi tietyn aiheen ympärillä käydyn keskustelun määrää, sävyä, näkökulmia ja ajoittumista verkosta kootussa aineistossa (esim. Fast-hakukoneen sovellukset). Tunnistuksen, paikannuksen ja tietovarastojen yhdistely seurantaan antaisi lisää mahdollisuuksia haluttujen toimien kohdistamiseen.

Sopivaan kohderyhmään kuuluminen, jonka mittareina voivat olla esimerkiksi ikä, sukupuoli, vuositulot, kulutuskäyttäytyminen, koulutus, asuminen, terveys, puoluekanta tai mielipiteet, tulee ubiikkiympäristössä vaikuttamaan yhä enemmän tarjolla oleviin palveluihin, etuuksiin, oikeuksiin ja rajoituksiin. Niiden vaikutukset voivat näkyä myös tiedonkeruussa poliittisia tarkoituksia varten. Mistä lähiöstä keskustelijat ovat kotoisin, kuinka paljon heitä on ja millaisia kuluttajia he ovat? Kannattaako heitä kuunnella? Kannattaisiko ikävää julkisuutta saanut hanke viedä läpi silloin, kun julkinen keskustelu asiasta on laantumassa?

Ubiikkiteknologian ympäristö on kansalaisen osallistumisen kannalta sekä hyödyllinen että vaarallinen. Se antaisi tehokkaammat välineet, joiden avulla olisi mahdollista seurata uutta tietoa sekä haluttujen kohteiden ja kohderyhmien toimia ja liikkeitä yhä tiiviimmin reaaliajassa. Ubiikkiteknologia voisi myös tehostaa vuorovaikutusta ja laajentaa osallistumisen ja vaikuttamisen käytäntöjä.

Kääntöpuolena välineet voivat tuottaa syvenevää kontrollia ja ohjailua. Kehittyneet tiedonhallinnan välineet antaisivat yrityksille ja viranomaisille seurata kansalaiskeskustelua ja puuttua siihen halutulla tavalla.

Kansalaisuuden ja demokratian toteuttamisen edellytykset

Mannermaa toteaa tulevaisuusvaliokunnalle tekemässään selvityksessä, että demokratian säilymisen kannalta on keskeistä huolehtia siitä, että ihmisillä itsellään pysyvät parhaimmat edellytykset, jotta he voisivat toimia kansalaisyhteiskunnan täysivaltaisina jäseninä (Mannermaa, 2007). Tämä edellyttää monipuolista tiedonsaantia, mutta myös osallistumisen ja vaikuttamisen mahdollisuuksia.

Internet-palveluilla ei sinänsä ole demokratisoivaa vaikutusta, jos yhteiskunnassa ei ole demokraattisia rakenteita ja sen säätelymekanismit ulottuvat verkkoon. Se voi jopa vahvistaa demokratian vastaisia toimia. (Kalathil, 2003, Kalathil & Boas, 2003).

Se, mitä ubiikkiyhteiskunnasta tulee erilaisissa yhteiskunnallisissa olosuhteissa, on edelleenkin teknologian ja politiikan yhteisvaikutusta. Huolestuttavaa onkin, että demokratian vastaiset käytännöt, kuten sensuuri, ovat viime vuosina levinneet eri maissa (Boyd, 2007).

Ubiikkiteknologian tuella kehitys on käymässä kohden kasvavan kontrollin yhteiskuntaa, johon sisältyy lähes täydellinen asioinnin, viestinnän ja liikkumisen seuranta. Valvonnan lisääntyminen ja tunnistuksen yleistyminen ja laajentuminen arkisten ympäristön toimiin kaventavat kansalaisen yksityisen ja anonyymin tilan.

Yksityisyyden, tietosuojan ja anonyymin asioinnin periaatteista tinkiminen toisi ubiikkiyhteiskuntaan tuntuvia haittavaikutuksia. Kansalaisen vaikuttamisen tila ja sen vaihtoehdot käytännössä vähenisivät. Näitä haittoja olisi mahdotonta paikata lisäämällä sisältöjen määrää, laajentamalla vuorovaikutteisuutta tai tuottamalla uudenlaisia välineitä.

> "Any form of interactivity that amounts to an unaccountable form of information gathering fails to live up to the promise of democratization." *(Andrejevic, 2007)*

Kansalaisen vaikutusvallassa verkossa ei ole kysymys vain ilmaisuvapaudesta, vaan ilmaisun tosiasiallisista ja ennakoitavista vaikutuksista. Sananvapauden muodollinen takaaminen ei riitä, jos viestintävälineiden rajoittavia käytäntöjä, tunnistusta ja tiedonkeruuta jatkuvasti laajennetaan. Välineiden puolesta vapaa sana, johon kuitenkin reagoidaan sekä reaaliaikaisten että elämänhistorian ajalta kertyneiden tietojen perusteella ennakoimattomissa yhteyksissä, rakentaa hyvin erilaisen yhteiskunnan kuin meillä on nykyisellään.

> "If, however, by participation we mean a conscious, considered, informed, and meaningful contribution to the governing process, it is important not to distinguish this at every turn from a version of participation that equates submission to detailed monitoring with participation." *(Andrejevic, 2007)*

Kansalaisyhteiskunnan raaka-aineeksi tarvitaan monipuolista tietoa ja keskustelua erilaisten näkemysten pohjalta. Miten tulisi käymään aidon kansalaiskeskustelun tiedonkeruun, tunnistuksen ja paikannuksen edetessä? Olisiko enää viisasta ottaa kantaa verkossa ja miten siellä ylipäänsä kannattaisi viestiä? Ubiikkiyhteiskunnassa ei kannattaisi erottua, jos siitä seuraisi epäedullinen profilointi tai merkintä poikkeavista mielipiteistä.

Jos todelliset mielenilmaisut eivät enää ole toivottavia, se on myös este innovaatioille. Paitsi demokratia, myös luovuus kukkii siellä, missä on mahdollista esittää monenlaisia ja ristiriitaisiakin näkemyksiä. Li-

sääntyvä valvonta tuo yhteiskuntaan pelon ilmapiirin, hyydyttää julkisen keskustelun ja kulttuurin ja pakottaa sen yhdenmukaisiin uomiin.

> "Surveillance comes with a price. It dulls the edge of public debate, imposes a sense of conformity, introduces the uneasy feeling of being watched. It chills culture and stifles dissent."
>
> *(O'Harrow, 2005)*

Käyttäjien vaikutusvalta verkkoyhteisöissä perustuu monipuoliseen tiedonsaantiin, anonyymiin viestintään ja mahdollisuuteen verkostoitua. Ilman näitä tekijöitä, verkon vapaus kaventuu oleellisesti. Läsnä- ja täsmäpalveluilla on kova hinta, jos se maksetaan kaventuneella puheella todellisuudesta.

Paratiisi vai panoptikon?

"Values are encoded in tecnology."

- Adam Greenfield, 2006

Matkalla kohden ubiikkiyhteiskuntaa verkkoympäristössä on tapahtumassa perustavaa laatua olevia muutoksia. Tarkentuva tunnistus, tietovarastojen laajentuminen ja avautuminen kansainväliseen käyttöön sekä älykkäiden teknologioiden yleistyvä hyödyntäminen kansalaisten seurantaan ja valvontaan on ilmeinen kehityksen suunta.

Ubiikkiteknologia voi avustaa uutisten, perheenjäsenten tai liikenteen seurantaa, mutta se edistää myös globaaliksi laajentuvia hallinnan ja valvonnan mahdollisuuksia. Ubiikkiympäristön rakentuminen globaaliksi toiminnallisuudeksi näkyy kehitteillä olevassa teknologiassa monelta osin – mm. IP-osoiteavaruuksissa, identiteetin metarakenteen valmistelussa, kansainvälisesti yhteensopivien sähköisten identiteettien kehittämisessä, kansallisten tietokantojen nopeassa laajentumisessa ja avaamisessa kansainväliseen käyttöön sekä satelliittipohjaisen ja langattoman verkon teknologioita hyödyntävän globaalin paikantamisen ja tunnistamisen rakentumisessa. Vain käyttäjät näyttävät olevan se osa infrastruktuuria, joilta vielä puuttuu käsitys koko ubiympäristön olemassaolosta (Greenfield, 2006).

Valvontayhteiskunnan kehittyminen näiden käytäntöjen varassa ei ole vain futuristinen uhkakuva, vaan sen etenemistä viime vuosina ovat monet asiantuntijat seuranneet. Lisääntyvä valvonta, tunnistamisen yleistyminen ja tarkentuminen biometrisiin menetelmiin, laajojen ja kansainväliseen käyttöön avautuvien tietokantojen rakentaminen antavat merkkejä johdonmukaisista askeleista kohden laajenevaa kontrollia

(Privacy international, 2007). Ubiikkiyhteiskunnan rakentuminen kietoutuu näihin käytäntöihin ja teknologioihin.

Privacy International -järjestön viimeisimmän vuosittaisen selvityksen mukaan, valvontayhteiskunnan ongelma ei ole vain sen nopeassa ja massiivisessa etenemisessä, vaan sen moninaisuudessa ja monimutkaisuudessa (Privacy international, 2007). Palaamme siis lähtöruutuun – koodin purkuun.

Kansalaiset ja päätöksentekijät tarvitsevat uutta lukutaitoa – hyvää käsitystä ubiikin teknologioiden toimintaperiaatteista, tiedonsiirroista, tietovarastoista, tietojen käyttötavoista sekä henkilöön liittyvän tiedonkäsittelyn vaikutuksista ja sen riskeistä. Samalla selviäisivät ne mahdollisuudet, joita voidaan käyttää kansalaisyhteiskunnan suojelemiseksi ja kansalaisen oikeusturvan säilyttämiseksi.

Ubiteknologia on haaste demokraattiselle vallankäytölle pienemmässä ja suuremmassa mittakaavassa. Konfliktiherkkyys, valvonnan kiristyminen, toimivallan siirtyminen uusiin käsiin sekä demokraattisen yhteiskunnan toimintaperiaatteiden rapautuminen muodostavat vakavan uhkakuvan yhteiskunnalle. Ubiikkiympäristö on myös entistä suurempien riskien ja väärinkäytösten ympäristö.

Tietojen ja teknologioiden väärinkäyttöön tulisi varautua. Tulisi myös estää sellaisen ympäristön ja toiminnallisuuden rakentuminen, joka johtaisi kansalaisten oikeusturvan vastaisiin käytäntöihin.

Ubiikkimaailma antaa sen tietovarastoja ja teknologioita hallitseville toimijoille laajentuvat valtuudet ja välineet suhteessa kansalaisiin. Vastapooliksi tarvittaisiin sen varmistamista, että kansalaisen oikeusturvan ja demokratian pelisääntöjä noudatetaan näiden valtuuksien käytössä. Tietosuoja on edelleen kansalaisen oikeuksien kannalta tärkeä asia.

Valvonnan tarkoituksenmukaisuutta ja laajentamista sekä pääsyn avaamista kansallisista tietojärjestelmistä kolmansille osapuolille pitäisi tarkasti harkita. Esimerkiksi teletunnistusjärjestelmän valvomiseksi on ehdotettu käytäntöä, jossa sen tosiasiallista ja tarkoituksenmukaista käyttöä, valvontaa ja tietoturvaa aika ajoin arvioitaisiin (Aarnio, 2005, EFFI 2007). Näin vältettäisiin tarpeettoman valvonnan ylläpitämistä tai sen laajentamista.

Kansalaisen askeleet kaikkialla tulevat julkisiksi sitä mukaa, kun ubiikkiteknologia leviää julkisiin tiloihin, kotitalouksiin, työpaikoille ja liikenteeseen. Läsnä- ja täsmä-äly tulee tiedonkeruun lisäksi seuraamaan, ohjaamaan, muistamaan ja muistuttamaan, suosittelemaan, valitsemaan, rajaamaan ja kieltämään ”kaikkialla” arkisessa ympäristössä.

Lähteet

2006/24/EY (2006), Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006 , yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta. (2006).
http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexdoc!prod!CELEXnumdoc&lg=FI&numdoc=32006L0024&model=guicheti

Aarnio, Reijo (2005), Teletietojen tallennusta arvioitava. Helsingin Sanomat, Pääkirjoitus, 1.11.2005.

Aktuellt (2007), A-kassan läser de arbetslösas bloggar. Aktuellt. 13.9.2007.
http://www.stoppa-storebror.se/aktuellt.htm

Ambient Displays Research Group.
http://www.eecs.berkeley.edu/Research/Projects/CS/io/ambient/

Andrejevic, Mark (2007), iSpy. Surveillance and power in the interactive era. University of Kansas, 2007.

Anti-chips.com. Anti-chipping legislation.
http://www.antichips.com/legislation.htm

Arora, Siddharira (2007), Review and analysis of current and future European e-ID card schemes. The 12th Porvoo Group Meeting, 18-19.10. 2007, Tuscany, Italy.
http://www.porvoo12.net/MSc_Information_Security.pdf

Autio, Antti (2006), Älykorttimarkkinoilla fuusiomylläkkä. Verkkouutiset, 23.5.2006.

BBC News (2005), Car charge trials ”in five years”. BBC News, 9.7.2005.
http://news.bbc.co.uk/1/hi/uk_politics/4075490.stm

Bellamy, Christine & Perri 6 & Raab Charles (2005), Personal data in the public sector: reconciling necessary sharing with confidentiality? In: Lace, Susanne (ed.) (2005), The glass consumer: life in a surveillance society.

Berteau, Stefan (2007), Facebook’s Misrepresentation of Beacon’s Threat to Privacy: Tracking users who opt out or are not logged in. CA Security Advisor Research Blog, 29.11.2007.
http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx

Borking, John (2005), The use and value of privacy-enhancing technologies. In: Lace, Susanne (ed.) (2005), The glass consumer: life in a surveillance society.

Björneborn, Lennart (2004), Small-world link structures across an academic web space : a library and information science approach. PhD dissertation. Royal School of Library and Information Science. xxxvi, 399 p. ISBN 87-7415-276-9 .
http://vip.db.dk/lb/phd/phd-thesis.pdf

Bottorff, Christian (2007), Technology scans for uninvited guests. Tennessean.com, 6.12.2007.
http://www.tennessean.com/apps/pbcs.dll/article?AID=/20071206/NEWS03/712060388/1001/RSS01

Boyd, Clark (2007), Internet Increasingly Censored. The first comprehensive global survey of Internet filtering shows that online repression is on the rise worldwide. Technology Review, 18.5.2007
http://www.technologyreview.com/Infotech/18749/?a=f

Brady, Brian (2008), Prisoners to be chipped like dogs. The Independent, 13.1.2008.
http://www.independent.co.uk/news/uk/politics/prisoners-to-be-chipped-like-dogs-769977.html

Business week (2004) Talking RFID with Wal-Mart's CIO (2004). Business week, February 4, 2004.
http://www.businessweek.com/technology/content/feb2004/tc2004024_3168_tc165.htm

Business week (2006), Background checks that never end. Business week, 20.3.2006.
http://www.businessweek.com/magazine/content/06_12/b3976065.htm

Canadian Cattle Identification Agency – About CCIA. [July 18, 2005].
http://www.canadaid.ca/About/#Description_and_Purpose

Castells, Manuell (1996), The Rise of the Network Society. The Information Age: Economy, Society, and Culture. Volume Internet. Cambridge.

CNN (2006), Brain chip heralds neurotech dawn. CNN, Monday, July 17, 2006.
http://www.cnn.com/2006/TECH/science/07/17/braingate.donoghue/index.html

CNN Europe (2007), Apology as data on millions lost. CNN Europe, November, 10, 2007.
http://edition.cnn.com/2007/WORLD/europe/11/21/britain.personal/index.html

CSC & Suomen yliopistojen ja korkeakoulujen ATK-keskukset (2004), HAKA-projektin loppuraportti. Johtopäätökset ja toimenpide-ehdotukset. 20.2.2004.
http://www.csc.fi/downloadPublication?uid=9bccf9982a6b38a272cb37c75322fbf4

Dean, Tony (2005), ITC475 Ethics and Technology Lectures, Charles Stuart University, School of Information Studies. ITC475 Lecture 5 Chp 5.
http://www.csu.edu.au/faculty/business/comp-math/subjects/itc475

Department of Commerce, National Science Foundation (2002), Converging technologies for improving human performance. June 2002. With assistance of World Technology Evaluation Center.
http://www.technology.gov/reports/2002/NBIC/Part1.pdf

Departements promemorian : Godkännande av Prümsbeslutet (2007). DS 2007:47.
http://www.datainspektionen.se/pdf/remissvar/2008-01-18-prumradsbeslutet.pdf

Dodig-Crnkovic, Gordana (2006), Investigations into Information Semantics and Ethics of Computing. A Doctoral Thesis, Department of Computer Science and Electronics. Mälardalen University, Västerås, Sweden. July 16th 2006.

DS 2007:47 (2007) Departements promemorian : Godkännande av Prümsbeslutet.
http://www.datainspektionen.se/pdf/remissvar/2008-01-18-prumradsbeslutet.pdf

Duris, Rick (2003), Just how big is RFID? RFID is a big deal. Its impact will be pervasive, personal and profound. It will be the biggest deal since Edison gave us the light bulb - Integrator's Notebook. Bnet Business Network –portal.
http://findarticles.com/p/articles/mi_m0DIS/is_12_4/ai_112366620

EFFI (2007), Lausunto liikenne- ja viestintäministeriön lausuntopyyntöön LVM036:00/2007 koskien luonnosta hallituksen esitykseksi Eduskunnalle laiksi sähköisen viestinnän tietosuojalain muuttamisesta (teletietojen tallennusvelvollisuus - isovelilaki). 31.7.2007.
http://www.effi.org/uutiset/070831-n-lausunto-viestintaminister.html

E-Europe Smart Cards Charter (2003), Electronic Identity (2003), White paper. eEurope Smart Cards. Trailblazer 1 "Public identity"

http://www.fineid.fi/vrk/fineid/files.nsf/files/
2F38FAA842A30AE5C225703F00253D8C/$file/eID-WP-final-o.pdf

Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006 , yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta. (2006).
http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexdoc!prod!CELEXnumdoc&lg=FI&numdoc=32006L0024&model=guicheti

Evans, Martin (2005), The data informed marketing model and its social responsibility. In: Lace, Susanne (ed.) (2005), The glass consumer: life in a surveillance society.

Fontana, John (2006), Setting the foundation for identity management, Network World, 03/20/06.
http://www.networkworld.com/supp/2006/ndc1/032006-ndc-identity-management.html?page=1

Fredrickson, Caroline (2008), The President is Trying to Legalize His Illegal Spy Program: Congress Should Just Say 'No'. ACLU – Americal Civil Liberties Union statement, 6.2.2008.
http://www.aclu.org/safefree/spying/34002leg20080206.html

Gaston, Lorenzo (2007), European citizen card going ahead. 11th Porvoo Group meeting, 24-25.5.2007, Coimbra, Portugal.
http://www.ama.pt/porvoo/apresentacoes/25_tarde/porvoo11_lorenzo_gaston.pdf

Goldman, Russell (2007), Do U.S. Companies Support Big Brother in China? ABC News. Science and Technology. 16.8.2007.
http://abcnews.go.com/Technology/story?id=3484293&page=1

Goodin, Dan (2007), Digital data can bite you in the ass, researcher warns, The Register, 22.6.2007.
http://www.theregister.co.uk/2007/06/22/protecting_data_usenix/

Greene, Kate (2008), TR10: Reality Mining. Technology Review, March/April 2008. MIT.
http://www.technologyreview.com/read_article.aspx?id=20247&ch=specialsections&sc=emerging08&pg=1

Greenfield, Adam (2006), Everyware: the dawning age of ubiquitos computing. Berkeley, California, New Riders, 2006.

Halkosaari, Antti (2007), Kameravalvonta muutoksessa. Laurea-ammattikorkeakoulu. Opinnäytetyö.
http://matu.laurea.fi/ep/tiedostot/ONTt/ONT_Halkosaari.pdf

Hall, Harriet (2005), Data use in credit and insurance: controlling unfair outcomes. In: Lace, Susanne (ed.) (2005), The glass consumer: life in a surveillance society.

HE 158/2007 vp (2007). Hallituksen esitys eduskunnalle laiksi sähköisen viestinnän tietosuojalain muuttamisesta.
http://www.eduskunta.fi/triphome/bin/vex3000.sh?TUNNISTE=HE+158/2007

HE 153/2006 (2006), Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä, laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain, pakkokeinolain 4 luvun, esitutkintalain 27 ja 28 §:n ja kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 ja 23 §:n muuttamisesta.
http://www.finlex.fi/fi/esitykset/he/2006/20060153

Heinonen, Risto (2001), Digitaalinen minä. Silta, Edita.

Holloway, Simon (2007), Real time location systems are the new buzz in RFID. The Register, 21.8.2007.
http://www.theregister.co.uk/2007/08/21/aeroscout_location_systems/

Honkanen, Mauri [et. el.] (2002), Ympäristö älykkäämmäksi. Prosessori, Marraskuu 2002.

Hämäläinen, Päivi (2005), Kansalliset hankkeet ja terveydenhuollon sekä sosiaalialan ja terveydenhuollon tietoteknologiakehitys. 21.1.2005.
http://www.kotu.oulu.fi/hyva/wellbe2/materiaali/Hamalainen.pdf

Inkinen, Sam (2004), Robo Sapiens: kyberkulttuurin utopioita ja dystopioita.
http://www.eisis.org/docs/robosapiens.pdf

Järvinen, Jani & Saarelainen, Ari (2007), Web-surffailuasi seurataan. Tietokone 13/2007.

Järvinen, Petteri (2007), Voiko nettikirjoituksilla vaikuttaa? Tietokone 13/2007.
http://www.pjoy.fi/lehdet/0713pj.htm

Kainulainen, Anssi (2005), Ryhmätietoisuutta tukevien jokapaikan tietotekniikan äänimaisemasovellusten arkkitehtuuri. Tampereen yliopisto, Tietojenkäsittelyopin pro gradu tutkielma, 2005.
http://tutkielmat.uta.fi/pdf/gradu00578.pdf

Kalathil, Shanti (2003), Dot Com for Dictators, Foreign Policy, Marc/April 2003.

Kalathil, Shanti & Boas, Taylor C. (2003), Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule. Washington D.C. Endowment for International Peace, 2003.

Karhula, Päivikki (toim.) (2001), Agentit tietotyön tukena. Eduskunnan kirjaston tutkimuksia ja selvityksiä 6. Helsinki, Eduskunnan kirjasto.

Karhula, Päivikki (2003). Eduskunnan kirjaston verkkopalvelustrategia 2003-2004. Eduskunnan kirjaston tutkimuksia ja selvityksiä 7.
http://lib.eduskunta.fi/dman/Document.phx?documentId=au30606140643809&cmd=download

Kasvi, Jyrki (2005), Kun yksityisyys kuoli. Blogi, 14.12.2005.
http://www.kasvi.org/index.php?id=506&cs=20

Kasvi, Jyrki (2006), Ei aseistettuja ulkomaisia turvallisuusjoukkoja Suomeen sopimuksen nojalla. Blogi, 30.5.2006.
http://www.kasvi.org/index.php?995

Kirves, Antti (2006), TV-ohjelma: Tuhansien korttitiedot kaupattiin Intiassa. Call Centerin työntekijät myivät. IT-viikko, 6.10.2006.
http://itviikko.fi/page.php?page_id=46&news_id=200617143

Klosek, Jaqueline (2007), The war on privacy. Praeger publishers, Westport.

Knuuttila, Oiva (2006), Ubicom –teknologiaohjelman ulottuvuudet. Seminaariesitelmä. UBICOM – jokapaikan tietotekniikka. TEKES. 3.5.2006.
http://akseli.tekes.fi/opencms/opencms/OhjelmaPortaali/ohjelmat/Ubicom/fi/Dokumenttiarkisto/Viestinta_ja_aktivointi/Seminaarit/Yhteisseminaari_030506/Knuuttila.pdf

Korpimies, Annika (2007). Operaattoreille vuoden tallennusnakki. Tietoviikko, 9.5.2007.
http://www.tietoviikko.fi/doc.te?f_id=1168709

Krim, Jonathan (2005), Online data gets personal: Cell phone records for sale. Washington Post, 7.7.2005.
http://www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070701862.html

Kuntaliitto & KUNTA-IT-yksikkö (2007), Kuntien työntekijöiden tunnistaminen ja käyttövaltuuksien hallinta VIRTU(K). Esiselvitys.
http://www.kunnat.net/attachment.asp?path=1;55264;122868;354;57710;124425;29746;29747;116762;124212

Lace, Susanne (ed.) (2005), The glass consumer: life in a surveillance society. Bristol, Policy.

Legge, Jessica (2008), WVHTC creating system to detect terrorist threats. http://www.timeswv.com/intodayspaper/local_story_024005932.html

Leidenius, Kim (2008), Henkilöstön seuranta lisääntyy. Tietokone 1/2008.

Lessig, Lawrence (2006), Code version 2.0. Basic books, New York. http://codev2.cc/

Liikenneministeriö (2006), Uusi arjen tietoyhteiskunta. Taustaselvitys Liikenneministeriölle. 10.4.2006. Arto Karila, Jukka Kemppinen, Mikko Kontiainen, Risto Kulmala, Esko Kurvinen, Martti Mäntylä, Antti Oulasvirta, Olli Pitkänen, Mika Raento, Antti Rainio, Antti Salovaara, Katri Sarkio, Risto Sarvas, Marko Turpeinen, Perttu Virtanen.
http://www.lvm.fi/oliver/upl236-Taustaselvitys.pdf

Linden, Mikael (2005), HAKA-infrastruktuuri käytössä syksyn alusta.
IT Universitas nro 8 / 2005.
http://www.yliopistojenit.fi/weblehti/nro8/linden.html

Linnake, Tuomas (2007), Verkon kalastelijat narrasivat 2,2 miljardia. Gatner tutki Yhdysvalloissa. Digitoday, 17.12.2007.
http://www.digitoday.fi/tietoturva/2007/12/17/Verkon+kalastelijat+narrasivat+2%2C2+miljardia/200732038/66

Mannermaa, Mika (2007), Demokratia tulevaisuuden myllerryksessä. Tulevaisuusvaliokunnan julkaisu. TUVJ 1/2007.
ISBN 978-951-53-2920-2 (nid.) ISBN 978-951-53-2921-9
http://www.eduskunta.fi/triphome/bin/thw.cgi/
trip?${APPL}=erekj&${BASE}=erekj&${THWIDS}=0.29/
496847&${TRIPPIFE}=PDF.pdf

Mannila, Marko (2007), Tietokannan ylläpitäjä myi 8,5 miljoonaa asiakastietoa. Digitoday, 3.12.2007. Ansaitsi yli puoli miljoonaa.
http://www.digitoday.fi/tietoturva/2007/12/03/Tietokannan+yll%E4pit%E4j%E4+myi+8%2C5+miljoonaa+asiakastietoa/200730674/66

Margulis, Stephen T. (2005), Privacy and psychology. Final draft. Paper to be presented at Contours of Privacy: Normative, psychological and social perspectives. November 5, 2005. Ottawa, Canada.
http://idtrail.org/files/Margulis_Contours.pdf

Mills, Elinor (2006), Google to censor China Web searches. CNET News.com, 24.1.2006.

http://www.news.com/Google-to-censor-China-Web-searches/2100-1028_3-6030784.html

Morville, Peter (2006): Ambient findability. Sebastopol, O'Reilly Media Inc.

Nakashima, Ellen (2007), FBI Prepares Vast Database Of Biometrics. Washington Post, 22.12.2007.
http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544_pf.html

Nieminen, Liisa (2007), Perusoikeuksien tulevaisuus Euroopassa. In: Euroopan tulevaisuus, Raunio Tapio & Saari, Juha (toim.). Helsinki, Gaudeamus.

Nivala, Mira (2007) ValtIT - Asiakaslähtöiset sähköiset palvelut kehittämisohjelma. Asiointitilin ja tavoitettavuustiedon kehittämistyö. Mira Nivala, 22.10.2007.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20071016ValtIT/04_SA_Asiointitilin_ja_tavoitettavuustiedon_kehittaeminen_22_10_2007_%5BVain_luku%5D.pdf

Nsanze, Fabienne (2004), ICT implants in the human body: a review. 21 December 2004. In: The ethical aspects of ICT implants in the human body. Proceedings of the round table debate. European Group on Ethics in Science and New Technologies to the European Commission, Secretariat of the EGE. Amsterdam, 21 December 2004.
http://ec.europa.eu/european_group_ethics/docs/roundtabict_en.pdf

O'Harrow, Robert, Jr. (2005), No place to hide. Free press. New York.

Olsson, Tobias (2008), Chefen ser dig – nytt program ska övervaka dina rörelser. Svenska dagbladet, 17.1.2008.

Ora, Janne (2006), Pekka Puska: KTL olisi luonteva ylläpitäjä, jos kansallinen DNA-rekisteri päätettäisiin luoda. Suomen lääkärilehti, 5/2006.
http://www.fimnet.fi/cl/laakarilehti/pdf/2006/SLL52006-405.pdf

Perri 6 (2005), The personal information economy: trends and prospects for consumers. In: Lace, Susanne (ed.) (2005), The glass consumer: life in a surveillance society.

Pienimäki, Tomi (2006), RFID and Finland Post. RFID:n hyödyntäminen postissa. Jokapaikan tietotekniikka –yhteisseminaari, EspooSeminaariesitys, [3.5.2006].
http://akseli.tekes.fi/opencms/opencms/OhjelmaPortaali/ohjelmat/Ubicom/fi/Dokumenttiarkisto/Viestinta_ja_aktivointi/Seminaarit/Yhteisseminaari_030506/Pienimaki.pdf

Poropudas, Timo (2007a), Joka kolmas hemmo urkkii yksityisasioita. Erikoisoikeudet kovassa käytössä. Digitoday, 30.5.2007.
http://www.digitoday.fi/tietoturva/2007/05/30/Joka+kolmas+ithemmo+urkkii+yksityisasioita/200713177/66

Poropudas, Timo (2007b), Pyllytatuointi voi tuhota työuran. Rekrytoijat seulovat tietoja yhteisöpalveluista. Digitoday, 15.6.2007.
http://www.digitoday.fi/page.php?page_id=66&news_id=200714935

Privacy International (2007), The 2007 International Privacy Ranking. Leading surveillance societies in the EU and the World 2007. 28.12.2007. Privacy International.
http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597

Privat, Ludovic (2008), Wayfinder launches location sharing application on Facebook. GPS Business News, 10.2.2008.
http://www.gpsbusinessnews.com/index.php?action=article&numero=648

[Prümin sopimus] (2007), Rajat ylittävän yhteistyön tehostamisesta erityisesti terrorismin, rajat ylittävän rikollisuuden ja laittoman muuttoliikkeen torjumiseksi Prümissa 27 päivänä toukokuuta 2005 Belgian kuningaskunnan, Saksan liittotasavallan, Espanjan kuningaskunnan, Ranskan tasavallan, Luxemburgin suurherttuakunnan, Alankomaiden kuningaskunnan ja Itävallan tasavallan välillä tehdyn sopimuksen täytäntöönpanosopimus.
http://www.finlex.fi/fi/sopimukset/sopsteksti/2007/20070055/20070055_2

Raab, Charles (2005), Regulatory provisions for privacy protection. In: Lace, Susanne (ed.) (2005), The glass consumer: life in a surveillance society.

Rainio, Antti (toim.) (2005), Älykkään liikenteen kehittämisstrategia vuosille 2005-2010. ITS Finland julkaisu 5/2005.
http://www.its-finland.fi/ITSFinlandStrategia2005.pdf

Ranjan, Jayanthi & Kamna, Malik (2007), Effective educational process: a data mining approach. Vine, Vol. 37, No. 4. 2007.

Rijnbende, Martin & Hamerlink, Thijas (2004), The future of shopping in Europe.
http://www.checkpointeurope.com/downloads/media/20040603101447Consumer_Survey.pdf

Rundle, Mary & Laurie, Ben (2005), Identity Management as a Cybersecurity Case Study Research Publication No. 2006-01, September 2005. The Berkman Center for Internet & Society at Harward Law School.
http://cyber.law.harvard.edu/home/uploads/521/2006_01_Rundle_IdentityManagement_CybersecurityCaseStudy.pdf

Savvas, Antony (2006), Police to store number plate data for at least two years. Computer weekly, 19.1.2006.
http://www.computerweekly.com/Articles/2006/01/19/213785/police-to-store-number-plate-data-for-at-least-two-years.htm

Sciannamea, Michael (2006), RFID Tag production on the rise.
The RFID Weblog. 24.1.2006.
http://www.instat.com/catalog/wcatalogue.asp?id=3#IN0502115WT

Singel, Ryan (2008), House Leaders Oppose Immunity, Reid Prepares For Extended Negotiations. Wired, 8.2.2008.
http://blog.wired.com/27bstroke6/2008/02/house-leaders-o.html

Sisäasiainministeriö (2003), EU-maat ottavat käyttöön Eurodac-järjestelmän. Tiedote, 13.01.2003.
http://www.intermin.fi/intermin/bulletin.nsf/PFBD/CE62DA0AF6EBC56EC2256CAD003DA692?opendocument

Sisäasiainministeriö (2005), Rajamäki: Päätös teletunnistetietojen tallentamisesta Suomen näkemyksen mukainen. Tiedote, 02.12.2005.
http://www.intermin.fi/intermin/bulletin.nsf/HeadlinesPublicFin/335E3CDB0B582BA3C22570CB00565FC4

Sosiaali- ja terveysministeriö (2003). Sähköisten potilasasiakirjajärjestelmien valtakunnallinen määrittely ja toimeenpano. Sosiaali- ja terveysministeriön työryhmämuistioita 2003:38.
http://www.stm.fi/Resource.phx/publishing/store/2004/01/pr1074496951603/passthru.pdf

Sosiaali- ja terveysministeriö (2004), Sähköisen potilasasiakirjan järjestelmien toteuttamista ohjaavan työryhmän loppuraportti. Sosiaali- ja terveysministeriön työryhmämuistioita 2004:18.
http://www.stm.fi/Resource.phx/publishing/store/2005/01/pr1105954774022/passthru.pdf

Sosiaali- ja terveysministeriö (2007), Biopankit, yhteinen etu ihmisperäisten näytekokoelmien hyödyntämistä, Sosiaali- ja terveysministeriön selvityksiä 2007:52.
http://www.stm.fi/Resource.phx/publishing/store/2007/10/pr1191577965530/passthru.pdf

SOU 2007:76 (2007) Lagring av trafikuppgifter for brottsbekämpning. Betänkande av trafikuppgiftsutredningen.

STT (2006a), KRP haluaa kansalaisista DNA-rekisterin, Helsingin sanomat, 26.1.2006.

http://www.hs.fi/kotimaa/artikkeli/Krp+haluaa+kansalaisista+dna-rekisterin/1135218506676

STT (2006b), Poliisiylijohtaja tyrmää koko kansan dna-rekisterin
Helsingin sanomat, 29.1.2006.
http://www.hs.fi/kotimaa/artikkeli/Poliisiylijohtaja+tyrm%C3%A4%C3%A4+koko+kansan+dna-rekisterin/1135218547213

Ström, Pär [2006], Människokartor ska följa oss meter för meter. Harry Potters magiska karta i verkligheten.
http://www.stoppa-storebror.se/optag.htm

Tenhunen, Emmi & Hämäläinen, Päivi & Kärki Jarmo & Väinälä, Anna (2006), Sosiaaliala ja sosiaali- ja terveydenhuollon tietoteknologiakehitys. Teoksessa Häyrinen Kristiina (toim.) Sosiaali- ja terveydenhuollon tietotekniikan ja tiedonhallinnan tutkimuspäivät. Tutkimuspaperit 2006. Työpapereita 18/2006, Stakes.
http://www.stakes.fi/verkkojulkaisut/tyopaperit/T18-2006-VERKKO.pdf

TEKES (2002). Tulevaisuus on osaamisessa. Teknologiastrategia – näkemys valinnoista.
http://www.tekes.fi/julkaisut/Teknologiastrategia.pdf. 5.8.2004.

TEKES (2006a), Ambience design: Creating multisensory environments. Project report.
http://akseli.tekes.fi/opencms/opencms/OhjelmaPortaali/ohjelmat/Sara/fi/Dokumenttiarkisto/Viestinta_ja_aktivointi/Muu_viestinta_ja_aktivointi/Projektiraportit/32_AmbienceDesign-reportx1x.pdf

TEKES, Suomen Akatemia (2006b), Finnsight 2015 : tieteen, teknologian ja yhteiskunnan näkymät : paneelien raportit. Helsinki, 2006.

Teräs, Arto (2005), Grid-verkostot perustuvat luottamukseen.
IT Universitas nro 8 / 2005.
http://www.yliopistojenit.fi/weblehti/nro8/teras.html

Thelwall, Mike (2007) Which types of news story attract bloggers? Vol. 12 No. 4, October 2007.
http://informationr.net/ir/12-4/paper327.html

Torpey, John (2000), The invention of the passport: surveillance, citizenship and the state. Cambridge University Press.

Valtionhallinnon IT-strategia (2006), 13.1.2006.
http://www.hare.vn.fi/upload/Asiakirjat/11289/84328_Valtiohallinnon_IT-strategia_130106_liitteineen.pdf

U 41/2007 vp. (2007), Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista.
http://www.eduskunta.fi/triphome/bin/vex3000.sh?TUNNISTE=U+41/2007

Valtionvarainministeriö (2006), Valtionhallinnon IT-strategia, 13.1.2006.
http://www.hare.vn.fi/upload/Asiakirjat/11289/84328_Valtiohallinnon_IT-strategia_130106_liitteineen.pdf

Valtionvarainministeriö (2007a), Virkamiehen tunnistaminen ja käyttöoikeuksien hallinta. Hankkeen esitutkimusraportti. Luonnos, 19.6.2007. Hallinnon kehittämisyksikkö.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070625Virkam/02_virtu_loppuraportti_1_0.pdf

Valtionvarainministeriö (2007b), KuntaIT-kehittäjäverkostojen muodostaminen. Hankkeen loppuraportti 20.11.2007. KuntaIT–yksikkö.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/04_hallinnon_kehittaminen/20071120KuntaI/512007.pdf

Wactlar, Howard D. & Cristel, Michael & Hauptmann, Alexander & Stevens, Scott (2003), A system of video information capture, indexing and retrieval for interpreting human activity. Carnegie Mellon University, School of Computer Science. Informedia –project.
http://www.informedia.cs.cmu.edu/documents/ispa03_wactlar.pdf

Vara, Vahini (2007), Facebook's Tracking of User Activity Riles Privacy Advocates, Members. Wall Street Journal, 21.11.2007.
http://online.wsj.com/public/article/SB119560466428899897.html

Washington Post (2000), Few Victims of Security Breaches Report Misuse of Data, Poll Shows, Washington post, November 10, 2000.
http://online.wsj.com/article/SB116308807315618655.html?mod=Harris+Poll

Yrjölä, Elina (2003), Siru kertoo, missä mennään. Talouselämä, 5.2.2003.
http://www.talouselama.fi/doc.te?f_id=429798

Sen anatomia on kuin verkkoon sisäänrakennettu sähköpaimen.

Anonyymiyden, yksityisyyden ja yksilön itsemääräämisoikeuden asteittainen katoaminen ja laajentuva vallansiirto ubimaailman hallinnoijille tuottavat myös merkittäviä perusoikeudellisia ongelmia kansalaisille, jos kehityksen suuntaan ei puututa. Yksityisyyteen ja anonyymiyteen liittyvät periaatteet ovat muuttumassa, tiedonkeruu ja tunnistuskäytännöt laajentumassa, valvonnan kynnys madaltumassa ja henkilöön liittyvä arviointi koventumassa. Onko se ubiikkiteknologian vai politiikan vaikutusta?

Ubiikkiympäristön raaka-ainetta ovat kansalaisia koskevat tiedot, joita kerätään ja yhdistellään yhä laajemmin. Ubimaailman keskeiset ristiriidat liittyvät näiden tietojen hallinnan ja omistuksen ympärille. Kansalaisen oikeusturvan kannalta keskeistä on kuitenkin huolehtia häneen liittyvien tietojen käsittelyn oikeuksista ja tietosuojasta.

> ”… the combination of international rules and emerging technology in identity management may inadvertently give government and the private sector an unprecedented amount of information on individuals in the networked world…The key is whether the system’s design enables citizens to maintain authority over government (or the powers acting in governmental capacities) and whether the design offers an individual effective recourse when his rights are not honored.” *(Rundle & Laurie, 2005)*

Yksityisyyden, anonyymiyden ja tietosuojan periaatteiden purkamisella on hinta. Ne kaventaisivat vapaan verkkomaailman ja purkaisivat kansalaisten perusoikeudet, mutta hävittäisivät myös ihmisyydestämme jotain oleellista ja arvokasta. Intiimiyden rajojen rikkominen hajottaa ihmisyyttä koossa pitävän tasapainon. Se todella tuo ontologisen ja olemuksellisen muutoksen, mutta onko se toivottava muutos?

Ubiteknologia on yhteiskunnan kannalta kriittistä teknologiaa, koska sillä rakennetaan uudenlaista infrastruktuuria. Ubiikkiympäristön riskit ja ongelmat tulevat suuremmiksi, niiden vaikutukset laaja-alaisemmiksi ja viimein peruuttamattomiksi, jos teknologian hyötyjä ja haittoja ei arvioida ajoissa rinnakkain. Nähdäänkö nyt riittävän hyvin, mitä ollaan rakentamassa ubiikkiyhteiskunnan infrastruktuuriin?

Koodi on lakia vahvempi

Jyrki Kasvi

Tietoyhteiskuntakehitys on ollut Suomessa viime vuosina nopeaa, mutta ei niinkään lainsäädännön tai viranomaisten ansiosta, vaan pikemminkin heistä huolimatta.

Viranomaiset ja poliitikot ovat jääneet pahasti teknologian kehityksestä jälkeen. Uusien tieto- ja viestintäteknologioiden läpimurtoon on havahduttu usein vasta silloin, kun niistä on jo ehtinyt tulla osa suuren kansalaisjoukon arkipäivää. Kehityksen ohjaaminen ja mahdollisten ongelmien ehkäiseminen on jälkikäteen kuitenkin vaikeaa, ellei mahdotonta.

Vaikka Suomi on ollut tietoyhteiskuntakehityksen edelläkävijämaa, uuden teknologian yhteiskunnallisia vaikutuksia ja lainsäädäntötarpeita on Suomessakin alettu pohtia vasta, kun teknisen infrastruktuurin perusta on jo rakennettu, ja uuden teknologian ympärille on kehittynyt oma sosiaalinen kulttuurinsa. Ja kun kulttuuri on syntynyt, sen muuttaminen edes lailla on hyvin vaikeaa.

Tekijänoikeuksien suojaaman musiikin, elokuvien ja tv-sarjojen laajamittainen jakelu Internetin vertaisverkoissa on tästä hyvä esimerkki. Vaikka uusi tekijänoikeuslaki teki tekijänoikeuden suojaamien teosten lataamisesta laitonta, teosten laajamittainen nettijakelu jatkuu edelleen.

Massojen piilokulttuuria verkossa

Tietoyhteiskunnan uusien trendien kehityskaari etenee usein samojen vaiheiden kautta. Aluksi uusi teknologia tai sosiaalinen ilmiö leviää netissä jopa vuosien ajan ilman, että perinteiset mediat tai poliittiset päättäjät kiinnittävät siihen juuri mitään huomiota. Ilmiön yhteiskunnallinen ja taloudellinen merkitys ehtii usein kasvaa todella suureksi, ennen kuin julkinen keskustelu sen merkityksestä käynnistyy perinteisissä tiedotusvälineissä.

Esimerkiksi nuorten suosimista virtuaalisista nettiyhteisöistä alettiin keskustella Suomessa vasta, kun IRC-Gallerialla oli käyttäjänään kokonaisia suomalaisten nuorten ikäluokkia. Tällä hetkellä 13-19-vuotiaista suomalaisista jo yli 60% on Galtsussa. IRC Gallerian, Facebookin, Twitterin ja Habbo Hotellin kaltaisista virtuaaliyhteisöistä onkin muo-

dostunut keskeinen osa uutta suomalaista nuorisokulttuuria ja nuorten sukupolvi-identieettiä.

Digitaalinen nuorisokulttuuri ei toki ole pelkästään suomalainen ilmiö. Esimerkiksi Suomessa kehitetyllä Habbo Hotellilla on eri puolilla maailmaa yhteensä 7,5 miljoonaa aktiivikäyttäjää, mikä tekee siitä maailman toiseksi suurimman virtuaalisen moninpeliyhteisön, heti 8,5 miljoonan pelaajan World of Warcraftin jälkeen. Habbo onkin yksi Suomen kansainvälisesti tunnetuimmista teknologia- ja kulttuurivientituotteista, jonka visuaalisesta ilmeestä on tullut osa globaalia pop-kulttuuria.

Vastaavasti nettirahapelien suosioon havahduttiin Suomessa vasta, kun 100.000 suomalaista jo pelasi pokeria ulkomaisilla pelipalvelimilla – Suomen rahapelimonopolien ja lainsäädännön ulottumattomissa. Nettipokeri on hyvä esimerkki Internetin kansallisen hallinnan vaikeudesta. Vaikka suomalaiset rahapelimonopolit eivät voi tarjota netissä rahapelipalveluita, se ei estä suomalaisia pelaamasta netissä rahapelejä jos ja kun heitä huvittaa.

100.000 suomalaisen nettiharrastuksen kieltäminen lailla on poliittisesti ja teknisesti vaikeaa. Vaikka kieltoihin päädyttäisiinkin, kansallisten rajoitusten kiertäminen on Internetissä hyvin helppoa. Kiellot johtaisivat todennäköisesti siihen, että nimenomaan nettipokeriaddiktit jatkaisivat pelaamista salassa, jolloin viranomaisten olisi entistä vaikeampi valvoa mahdollisia väärinkäytöksiä ja ehkäistä peliaddiktion haittoja. Suomalaisten nettipokeripalvelinten perustaminenkin voi olla jo liian myöhäistä, sillä nimenomaan aktiivipelaajat ovat jo tottuneet pelaamaan ulkomailla.

Välinpitämättömyydestä mediapaniikkiin

Median ja poliitikkojen havahtuminen tietoyhteiskunnan uusiin ilmiöihin tapahtuu usein rytinällä. Tiedotusvälineet nostavat julkisuuteen jonkin yksittäisen ilmiön, joka hämmentää ja järkyttää suurta yleisöä ja aktivoi poliitikkojen lausuntoautomaatin. Esimerkiksi nuorten nettiyhteisöistä käyty keskustelu on keskittynyt lähinnä tyttöjen netissä julkaisemien herutuskuvien päivittelyyn ja netissä teineiksi tekeytyvien keski-ikäisten pedofiilien kauhisteluun. Samalla satojentuhansien nuorten digitaalinen arki on leimattu turhanaikaiseksi, jopa vaaralliseksi puuhasteluksi.

Mediakohun myötä poliitikoilta vaaditaan pikaisia toimenpiteitä, kieltoja ja rajoituksia uhkakuvien torjumiseksi. Päätöksentekijät eivät kuitenkaan läheskään aina ymmärrä, mistä uusissa ilmiöissä oikein on kyse, ja millaiset rajoitukset ovat ylipäätään teknisesti mahdollisia.

Esimerkiksi Suomen rahapelimonopolien suojaamiseksi esitettiin, että Suomesta tulisi estää pääsy ulkomaisille nettipokeripalvelimille. Estoon olisi käytetty lapsipornon ennakkosensurointiin käytettävää kansallista sulkulistaa, jonka sisältö on salainen, ja josta ei voi valittaa. Pitävä esto osoittautui kuitenkin perustuslain kannalta ongelmalliseksi ja mahdottomaksi toteuttaa aukottomasti.

Joskus uhkakuvia rakennetaan myös tarkoituksellisesti. Vuonna 1985 eduskunnassa tehtiin Raid Over Moscow -tietokonepelistä hallitukselle kirjallinen kysymys, koska kyseisen pelin pelättiin vaarantavan suhteet Neuvostoliittoon ja murentavan rauhankasvatusta. Tapaus on hyvä esimerkki siitä, miten hyökkäykset uutta digitaalista kulttuuria vastaan usein vain vahvistavat sitä. Mediakohun myötä keskinkertaisesta pelistä tuli poikkeuksellisen suosittu, ja se pysyi myyntitilastojen kärjessä useiden kuukausien ajan.

Lapset ja nuoret ovat omaksuneet uudet teknologiat ensimmäisinä ja törmäävät ensimmäisinä myös niiden mahdollisiin haittoihin. Monille aikuisille uudet teknologiat ja niiden ympärille syntynyt nuorisokulttuuri ja sosiaaliset ilmiöt ovat sen sijaan vieraita, eivätkä he osaa olla vanhempia lapsilleen tällä elämänalueella. Vanhemmat eivät ymmärrä, että nykymaailmassa on aivan yhtä tärkeää varoittaa lastaan tapaamasta uutta nettituttavuutta yksin kuin kieltää häntä nousemasta vieraaseen autoon.

Vanhempien kannalta tilanteen tekee erityisen vaikeaksi se, että tuoreen Eurobarometri-tutkimuksen mukaan lapset ja nuoret välttävät vanhempiensa puoleen kääntymistä viimeiseen asti kohdatessaan netissä ongelmia. Lapset pelkäävät vanhempiensa säikähtävän ja rajoittavan heidän netin käyttöään. Siksi vakavistakin ongelmatilanteista ennemmin vaietaan, sillä netti on keskeinen osa nuorten sosiaalista pääomaa. Netin käytön rajoittaminen koetaan lähinnä pysyväksi kotiarestiksi, epäreiluksi rangaistukseksi siitä, että on joutunut netissä väärinkäytöksen uhriksi.

Mediapaniikin ja ylilyöntien jälkeen viranomaisille ja poliitikoille kuitenkin vähitellen valkenee uuden ilmiön taloudellinen ja yhteiskunnallinen merkitys. Pian siihen liittyvän uuden teknologian kehittämistä aletaan tukea myös taloudellisesti. Esimerkiksi aiemmin lasten ja nuorten turmelemisesta syytetty tietokonepeliteollisuus saa nykyään tuotekehitysrahaa Tekesiltä. Suomen yliopistoissa on myös useita pelien maailmaan keskittyviä tutkimus- ja koulutushankkeita.

Todennäköisesti nettirahapelien kehitystyötäkin aletaan lähitulevaisuudessa tukea veronmaksajien rahoilla. Etenkin kännyköillä pelattavat

mobiiliuhkapelit ovat osoittautuneet todelliseksi läpimurtopalveluksi, eivätkä suomalaiset halua jäädä niillä markkinoilla pelkiksi asiakkaiksi ja maksajiksi.

Teknologia käy lainsäädännön edellä

Perinteinen lainsäädäntöprosessi on tietoyhteiskuntakehityksen tahdille aivan liian hidas. Teknologian kehitys ei pysähdy odottamaan, kun työryhmä laatii mietinnön, asianosaiset antavat lausunnot, ministeriö valmistelee esityksen ja eduskunta säätää lain. Uutta teknologiaa koskevat lait ovatkin usein jo syntyessään vuosia ajastaan jäljessä.

Hyvän esimerkin tarjoaa äskettäin voimaan tullut modeemikaappauslaki, jota olisi tarvittu jo 10 vuotta sitten. Nyt se on kuitenkin auttamattoman vanhentunut. Kenellä ylipäätään on enää modeemi, jonka joku voisi kaapata? Sen sijaan tarvittaisiin lainsäädäntöä, joka tukisi tietoturvaviranomaisten työtä botnettien torjunnassa.

Uusia teknologioita koskevan lainsäädännön perusongelmana on se, että laki ei voi olla ristiriidassa laajassa käytössä olevan teknologian kanssa. Koska tieto- ja viestintäteknologia kehittyy lainsäädäntöä nopeammin, olemassa oleva teknologia asettaa käytännössä rajat sille, millainen lainsäädäntö on mielekästä ja millainen ei. Moni tieto- ja viestintätekniikkaa koskeva lakipykälä onkin jäänyt kuolleeksi kirjaimeksi, koska sen toimeenpano ja valvonta on joko mahdotonta tai tulisi ainakin hyvin kalliiksi. Lawrence Lessigiä mukaillen voidaan sanoa, että koodi on lakia vahvempi.

Usein kuulee esimerkiksi vaadittavan, että nettikeskusteluilta tulisi lailla edellyttää vastaavaa päätoimittajaa ja puheenvuorojen ennakkotarkastusta. Mutta mitä pitäisi tehdä esimerkiksi Usenet-keskusteluille, jotka sijaitsevat fyysisesti kaikkialla mutta eivät missään, ja joista kukaan ei ole vastuussa? Yhtä järkevää olisi vaatia ihmisiä tankkaamaan autonsa tankkiin maitoa bensan asemesta. Sitä paitsi nettikeskusteluja on ylipäänsä niin paljon, että niiden kattava ennakkovalvonta on yhtä mahdotonta kuin kaikissa Suomen kahviloissa käytyjen keskusteluiden seuranta ja sensurointi.

Digitalisoituminen pakottaa uusimaan myös medioita säätelevän lainsäädännön rakenteita. Tähän asti eri medioita on säädelty erillisillä laeilla, mutta kun kaikkia sisältöjä käsitellään digitaalisesti, medialla ei ole enää merkitystä. Internetin näkökulmasta elokuvalla, sinfonialla, nettisivulla ja tietokoneohjelmalla ei ole mitään eroa. Kaikki ovat bittejä tietoverkossa, ja kaikkia käsitellään samalla tavalla.

Medioiden digitalisoitumisen seurauksena eri medioita koskevaa lainsäädäntöä on pakko yhtenäistää. Kun esimerkiksi uudesta tekijänoikeuslaista rajattiin ohjelmistot ja tietokannat pois, tuloksena oli laki, jonka mukaan ohjelmistojen ja tietokantojen välittäminen tietoverkoissa on laitonta.

Tekijänoikeuslain 11 a § kun sallii tilapäisten kopioiden tekemisen Internetin reitittimissä, jotta teosten siirtäminen tietoverkoissa olisi mahdollista. Tästä poikkeuksesta rajataan kuitenkin tietokoneohjelmat ja tietokannat erikseen ulos:

> Mitä 2 §:ssä säädetään oikeudesta valmistaa teoksesta kappaleita, ei koske sellaista tilapäistä kappaleen valmistamista:
>
> 1) joka on väliaikaista tai satunnaista
> 2) joka on erottamaton ja välttämätön osa teknistä prosessia
> 3) jonka ainoa tarkoitus on mahdollistaa välittäjän tekemä teoksen siirto verkossa kolmansien osapuolten välillä tai teoksen laillinen käyttö; sekä
> 4) jolla ei ole itsenäistä taloudellista merkitystä.
>
> Mitä 1 momentissa säädetään, ei sovelleta tietokoneohjelmaan eikä tietokantaan.

Suomessa myös tietokoneohjelmistot kuuluvat tekijänoikeuden piiriin, toisin kuin tekijänoikeusdirektiivin esikuvana toimivassa Yhdysvalloissa, jossa ohjelmistot suojataan patenteilla. Eurooppalaisen ohjelmistoteollisuuden immateriaalioikeudet ovatkin jääneet väliinputoajan asemaan.

Lainulkopuoliset käytännöt

Sähköisen viestinnän tietosuojalaissa on vastaava ongelma. Laki kieltää tunnistetietojen ja päätelaitteen sijaintitiedon – eli laissa käytetyllä käsitteistöllä paikkatiedon – käsittelyn muuten kuin erikseen määriteltyjä tarkoituksia varten. Tunnistetietojen kohdalla nämä tarkoitukset ovat palvelun toteuttaminen ja käyttäminen, laskutus, markkinointi, tekninen kehittäminen, väärinkäytösten selvittäminen, teknisten vikojen ja häiriöiden havaitseminen sekä käsittelytietojen tallentaminen (ks. Sähköisen viestinnän tietosuojalain 3. luku). Sen sijaan sijaintitietoja saa lain neljännen luvun mukaan käyttää vain ja ainoastaan palvelun toteuttamiseksi ja käyttämiseksi. Edes väärinkäytösten selvittämiseen tai teknisten vikojen havaitsemiseen niitä ei siis saa käyttää.

Käytännössä tietokoneohjelmia ja tietokantoja välitetään edelleen tietoverkoissa ja päätelaitteiden sijaintitietoja käytetään virhetilanteiden selvittämiseen ja palveluiden kehittämiseen siinä missä muitakin tunnistetietoja. Sanotaan laissa mitä tahansa. Muuten koko Internet lakkaisi toimimasta, sisältöbisnes kuihtuisi, eikä paikkatietopalvelujen kehittäminen ja ylläpito olisi mahdollisia.

Lainsäädännön ristiriitaisuus ja mahdottomat lakipykälät hämmentävät uusien tietoyhteiskuntapalveluiden kehittäjiä. He joutuvat pykälä pykälältä itse arvioimaan, mitkä lakipykälät pitää ottaa vakavasti ja mistä pykälistä ei tarvitse välittää. Yksiselitteistä ohjelmakoodia kirjoittamaan tottuneen insinöörin on vaikea käsittää lakeja, jotka ovat näin tulkinnanvaraisia ja ristiriitaisia. Ei ole mikään ihme, jos myös vakavasti otettavaksi ja noudatettavaksi tarkoitettujen pykälien kunnioitus joskus unohtuu.

Usein jopa viranomaiset joutuvat katsomaan toiseen suuntaan, kun laki haittaa tietojärjestelmien ylläpidolle välttämätöntä toimintaa. Esimerkiksi haittaohjelmien ja roskapostien tehokas suodatus sähköpostiliikenteestä on käytännössä mahdotonta, jos kaikkien viestien sisältöjä ei analysoida automaattisesti. Sähköisen viestinnän tietosuojalain mukaan viestin sisällön saa kuitenkin analysoida vasta, jos on todennäköisiä syitä esimerkiksi viestin tunnistetietojen perusteella epäillä viestin sisältävän haittaohjelman tai roskapostia:

> Viestin sisältöön saa puuttua ainoastaan teknisin keinoin viestin tarkastamiseksi ja poistamiseksi, jos on todennäköisiä syitä epäillä viestin sisältävän sellaisen tietokoneohjelman tai ohjelmakäskyjen sarjan, jota tarkoitetaan rikoslain (39/1889) 34 luvun 9 a §:n1 kohdassa tai jos on todennäköisiä syitä epäillä, että viestiä käytetään rikoslain 38 luvun 5 § :ssä säädettyyn tietoliikenteen häirintään. (Sähköisen viestinnän tietosuojalaki 20 §)

Käytännössä tätä ehtoa ei tietenkään noudateta, ei edes lain säätäneessä eduskunnassa. Perusteluna on se, että koska suurin osa sähköpostiliikenteestä on roskapostia, kaikkia viestejä voidaan todennäköisin syin epäillä roskaposteiksi tai haittaohjelmiksi.

Suomen tieto- ja viestintätekniikkaa koskevassa lainsäädännössä on toki myös onnistuneita kohtia. Esimerkiksi sähköisen viestinnän tietosuojalaissa teleyritykset velvoitetaan pitämään lokia keräämiensä tunnistetietojen käsittelystä. Taannoisen Sonera-skandaalin tutkinnan yhteydessä kun kävi ilmi, miten vaikeaa tunnistetietojen väärinkäyttöä on todistaa, jos niiden käsittelystä ei jää mihinkään mitään merkintää:

> Teleyrityksen on tallennettava tunnistamistietojen käsittelystä yksityiskohtaiset tapahtumatiedot. Tapahtumatiedoista on käytävä ilmi käsittelyn ajankohta, kesto ja käsittelijä. Tapahtumatiedot on säilytettävä kaksi vuotta niiden tallentamisesta. (Sähköisen viestinnän tietosuojalaki 15 §)

Saman periaatteen soisi leviävän myös muihin kansalaisten tietoja sisältäviin tietokantoihin.

Tietotekniikkayrityksissä on onneksi opittu lukemaan alan lainsäädäntöä luovasti. Jos yrityksissä noudatettaisiin lakipykäliä samalla tarkkuudella kuin tietojärjestelmien määrittelydokumentteja, moni palvelu olisi jäänyt oikeustoimien pelossa kehittämättä. Kalliiden väärinymmärrysten välttämiseksi insinöörien ja juristien on pakko oppia puhumaan samaa kieltä. Joka tapauksessa juristeilla, jotka ymmärtävät myös tietotekniikkaa, on lähivuosina paljon kysyntää.

Miten voi ymmärtää tekijänoikeuslainsäädäntöä?

Viime vuosina on keskusteltu erityisesti tiedonvälityksen digitalisoitumisen tekijänoikeustaloudelle aiheuttamista ongelmista. Digitaaliseen tiedon käsittelyyn on siirrytty nimenomaan siksi, että digitaalisen tiedon virheetön käsittely: Tallennus, kopiointi ja välittäminen ovat helppoa ja halpaa, käytännössä ilmaista. Samalla mediateollisuuden vanhat, analogiseen teknologiaan perustuneet bisnesmallit ovat kuitenkin joutuneet kriisiin. Kuluttajien tarpeet ja mediateollisuuden tuotteet eivät aina enää kohtaa.

Mediateollisuus on pyrkinyt suojaamaan etujaan estämällä tuotteidensa kopioinnin erilaisilla kopiosuojaustekniikoilla. Niiden kiertäminen on kuitenkin osoittautunut hyvin helpoksi, koska vahva suojaus edellyttäisi soittimilta niin paljon laskentatehoa, että soitinten hinta nousisi kohtuuttoman kalliiksi. Suojaus kun on joka tapauksessa pakko purkaa, jotta musiikkia tai elokuvaa tai muuta sisältöä pystytään käyttämään.

Kuluttajat haluaisivat hyödyntää uuden tieto- ja viestintäteknologian suomia mahdollisuuksia, mutta mediateollisuus kokee ne uhaksi liiketoiminnalleen. Tämän ristiriidan seurauksena suuri joukko suomalaisia rikkoo jatkuvasti lakia esimerkiksi ottaessaan Internetistä ostamistaan musiikkitiedostoista varmuuskopioita.

Tiedostojen kopiosuojauksen (eli ns. tehokkaan teknisen toimenpiteen) kiertäminen ja kiertämiseen käytetyt apuohjelmat ovat laittomia, mutta ilman niitä satojen eurojen arvoisen mp3-musiikkikokoelman siir-

täminen uudelle mp3-soittimelle ei ole mahdollista. Ja ilman varmuuskopioita mp3-soittimen tai tietokoneen rikkoutuminen tuhoaisi netistä ostetut musiikkitiedostot peruuttamattomasti. Kuluttajan olisi pakko ostaa ne itselleen uudelleen.

> Tehokkaan teknisen toimenpiteen kiertämisen mahdollistavia tai kiertämistä helpottavia laitteita, tuotteita tai osia ei saa valmistaa tai tuoda maahan yleisölle levittämistä varten, levittää yleisölle, myydä, vuokrata, mainostaa myytäväksi tai vuokrattavaksi eikä pitää hallussa kaupallisessa tarkoituksessa. Tehokkaan teknisen toimenpiteen kiertämisen mahdollistavia tai sitä helpottavia palveluja ei liioin saa tarjota. (Tekijänoikeuslaki 50b §)

Usein kuluttajat myös kokevat, etteivät he saa haluamaansa palvelua, ja ovat siksi valmiita rikkomaan lakia. Monet esimerkiksi haluavat seurata amerikkalaisia tai japanilaisia TV-sarjoja, joita ei Suomessa esitetä, tai jotka esitetään Suomessa alkuperäisiä teknisesti huonolaatuisempina. Netistä sarjat ovat kuitenkin imuroitavissa samana päivänä kun ne esitetään Yhdysvalloissa, HD-laatuisella kuvalla ja monikanavaisilla äänillä. Useimmat eivät koe edes tekevänsä mitään väärää, koska laillista tapaa kyseisten sisältöjen ostamiseen ei vielä ole olemassa.

Nykyinen tekijänoikeusjärjestelmä syntyi kirjapainotekniikan leviämisen seurauksena, heikoimman osapuolen eli tekijän suojaksi julkaisijoiden eli kirjankustantajien toimintaa vastaan. Digitaalinen tiedon välitys luo kuitenkin uusia tarpeita. Tarvitsevatko esimerkiksi julkaisijat eli mediateollisuus suojaa kuluttajien toimintaa vastaan vai pitääkö kuluttajia päinvastoin suojella mediateollisuuden toimilta?

Perinteisten tekijänoikeuksien rinnalle on syntynyt myös uusia, Internet-kulttuurin tarpeisiin vastaavia lisenssejä, joiden avulla sisällöntuottajat voivat määritellä, mitä käyttäjät saavat heidän tuottamalleen aineistolle tehdä. Erilaiset Copyleft-lisenssit kuten BSD, GPL ja Creative Commons antavat sisältöjen käyttäjille tavanomaista tekijänoikeutta enemmän oikeuksia. Käyttäjille ne kuitenkin muodostavat sekavan viidakon, jonka pelisääntöjä on vaikea hahmottaa.

Lisenssin yksityiskohdista riippuen sisältöä voi esimerkiksi käyttää vapaasti, mutta ei muuttaa, kunhan alkuperäisen tekijän nimi mainitaan. Toinen lisenssi saattaa puolestaan antaa luvan muuttaa teosta, kunhan myös tuloksena olevaa teosta saa muuttaa vapaasti. Tekijänoikeuslainsäädäntöä kehitettäessä tulisikin huomioida myös nämä uudet, tekijänoikeutta väljemmät lisenssit.

Yhteisöllinen ja henkilökohtainen media haastaa käsitteet

Internetin vuorovaikutteiset sosiaaliset mediat kasvattavat suosiotaan ja haastavat sekä perinteiset valtamediat että lainlaatijat. Tiedotusvälineitä säätelevä lainsäädäntö on luotu keskitettyjen, yksisuuntaisten medioiden maailmaan, maailmaan, jossa on painokoneita ja radiolähettimiä, joiden käyttöä valvotaan ja kontrolloidaan. Maailmaan, joissa tiedotusvälineillä on sisällöstä vastaava päätoimittaja.

Tietoverkoissa perinteinen median sääntely ei toimi, sillä kuka tahansa voi harjoittaa joukkoviestintää. Joukkoviestintään ei tarvita painokoneen kaltaisia kalliita investointeja, pelkkä nettiyhteys ja osoite webhotellissa riittävät. Esimerkiksi suosituimmilla suomalaisilla blogeilla on tuhansia lukijoita joka päivä, samoin lukijoiden kirjoittamilla kommenteilla.

Keskitettyjen medioiden perinne näkyy hyvin niissä puheenvuoroissa, joissa vaaditaan Internetin sisällön ennakkosensuuria ja Internet-operaattoreita vastuuseen Internetin sisällöstä eli siitä, mitä ihmiset nettisivuillaan julkaisevat ja keskustelupalstoilla kirjoittavat. Aivan kuin nettipalvelin olisi operaattorin hallitsema radiolähetin tai painokone. Samalla logiikalla Itella tulisi asettaa vastuuseen postinkantajien ihmisten postilaatikoihin kantamien lehtien sisällön laillisuudesta, tai Digia Yleisradion ohjelmien arvomaailmasta.

Netissä kuka tahansa voi osallistua myös yhteisiin julkaisuhankkeisiin, kansalaismedioihin, joista tunnetuin on tammikuussa 2001 perustettu Wikipedia, kansainvälinen verkkotietosanakirja, jonka hakusanoja kuka tahansa voi kirjoittaa ja muokata. Tällä hetkellä Wikipedia on yksi maailman 10 suosituimmasta sivustosta, jossa on jo noin 8,5 miljoonaa Wikipedian lukijoiden kirjoittamaa artikkelia yli 250 kielellä.

Mutta kuka on vastuussa Wikipedian kaltaisten hajautettujen projektien tuloksista? Kuka ne omistaa? Kuka vastaa esimerkiksi Wikipediaan yhdessä kirjoitetusta artikkelista, jos se loukkaa jonkun kunniaa? Entä yhteisprojektien talous? Ovatko esimerkiksi lukijoiden kansalaismedioiden sisällöntuottajille vapaaehtoisesti maksamat palkkiot rahankeräystä vai liiketoimintaa? Entä open source -ohjelmien kehittäjille annetut mikrolahjoitukset?

Paikkatiedon epäselvät pelisäännöt

Hyvän esimerkin lainsäädännön ja uuden tieto- ja viestintäteknologian ristiriidasta tarjoaa paikka- ja sijaintitietoa koskevan lainsäädännön sekavuus. Jopa lakien käsitteistö on epäyhtenäistä vaihtuen laista toiseen.

Päätelaitteen sijainnin kertovasta tiedosta eli sijaintitiedosta käytetään kolmessa eri laissa kolmea eri nimeä: Paikkatieto (sähköisen viestinnän tietosuojalaki), paikantamistieto (meripelastuslaki) ja sijaintitieto (rajavartiolaitoslaki). Laissa geodeettisesta laitoksesta ja maanmittauslaitoksesta paikkatieto-sanalla on kuitenkin oikea merkitys. Siinä sanalla paikkatieto tarkoitetaan nimenomaan kiinteää paikkaa koskevaa tietoa mobiilin päätelaitteen sijaintitiedon asemesta.

Sähköisen viestinnän tietosuojalaki on ainoa, jossa paikkatieto määritellään, ja siinäkin määritelmä on siis väärä, sillä kyse on sijaintitiedosta:

> ”…paikkatiedolla tietoa, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun tarkoitukseen kuin verkkopalvelun tai viestintäpalvelun toteuttamiseen…”
>
> *Sähköisen viestinnän paikkatietolaki, § 2*

Tieto- ja viestintäalalle tarvittaisiinkin oma insinööri-juristi-käännösohjelma, joka auttaisi uusien tietojärjestelmien kehittäjiä lukemaan ja ymmärtämään oman alansa lainsäädäntöä.

Paikka- ja sijaintitiedot ovat arjen tietoyhteiskunnan ubiikkipalveluiden kehittämisessä aivan keskeisessä asemassa. Uusia paikka- ja sijaintitietoja hyödyntäviä laitteita ja palveluita tulvii markkinoille, mutta lainsäädäntö ja pelisäännöt puuttuvat. Edes tuore kansallinen paikkatietostrategia ei kiinnitä alan lainsäädännön kehittämistarpeisiin mitään huomiota.

Kuka saa esimerkiksi tuottaa ja hallita paikkatietoa? Kuka omistaa verovaroilla tuotetut paikkatiedot ja millä ehdoilla niitä voidaan hyödyntää kaupalliseen ja epäkaupalliseen toimintaan? Mistä mahdollisia maksuja saa kerätä: Pääsystä paikkatietoon, paikkatiedon käyttämisestä vai sen varaan rakennetusta palvelusta?

Etenkin paikkatietojen käytön hinnoittelulla on suuri merkitys, sillä epätarkoituksenmukaiset maksut voivat estää uusien innovatiivisten paikkatietopalveluiden kehittymisen. Esimerkiksi Yhdysvalloissa verovaroin tuotetut paikkatiedot ovat ilmaiseksi kaikkien käytettävissä, mikä on nopeuttanut erilaisten paikkatietopalvelujen kehitystä. Uusien paikkatietopalveluiden tuoton verottaminen tuo yhteiskunnalle paljon enemmän varoja kuin raakadatan käytöstä perittävät maksut.

Vastaavasti myös päätelaitteiden sijaintia koskevien sijaintitietojen hallinta vaatii selkeitä pelisääntöjä. Millä ehdoilla operaattorit saavat luovuttaa tiedot päätelaitteiden sijainnista kaupallisiin tarkoituksiin? Kuka omistaa tiedon henkilön sijainnista? Ovatko sijaintitiedot julkisia vai yksityisiä?

Ihmisille voi tulla tarve jopa väärän sijaintitiedon levittämiseen. Kaikki eivät välttämättä aina halua antaa perheelle ja ystäville oikeaa tietoa omasta sijainnistaan. Saako teleoperaattori tarjota myös tällaista palvelua?

Puuttuva keskustelu kansalaisoikeuksista

Tietoyhteiskuntakehitys pakottaa meidät kyseenalaistamaan ja arvioimaan uudelleen itsestään selvinä pitämiämme kansalaisoikeuksia ja -vapauksia. Tämä keskustelu on Suomessa edelleen käymättä, mutta silti esimerkiksi Kansallisessa tietoyhteiskuntastrategiassa (2007-2015) kansalaisoikeuksia ei mainita sanallakaan!

Kansalaisoikeudet ovat demokratian ydin. Demokratiaa ei voi olla ilman sananvapautta ja yksityisyyden suojaa. Siihen kuuluu myös anonymiteetti. Oikeus hankkia tietoa vapaasti ja ilman pelkoa. Oikeus ilmaista mielipiteensä vapaasti ja ilman pelkoa siten, että viranomaiset eivät tiedä, kuka mitäkin tietoa hankkii ja kuka minkäkin mielipiteen ilmaisee.

Anonymiteetti on nettiviestinnässä sama asia kuin naamioitumisoikeus mielenosoituksissa:

> Viesti ei ole luottamuksellinen, jos se on saatettu yleisesti vastaanotettavaksi. Viestiin liittyvät tunnistamistiedot ovat kuitenkin luottamuksellisia. (Sähköisen viestinnän tietosuojalaki 4 §)

Nyky-Suomessa näin vahva yksityisyyden suoja saattaa tuntua liioittelulta. Historia on kuitenkin opettanut, että kun viranomaisilla on ollut mahdollisuus seurata ihmisten tiedon hankintaa ja mielipiteen ilmaisua, sitä mahdollisuutta on ennemmin tai myöhemmin myös käytetty ihmisten mielipiteiden kontrolloimiseen. Suomalaisten nykyiset kansalaisoikeudet ovat valitettavan harvinainen poikkeus maailmassa.

9.11.2001 jälkeisessä maailmassa sananvapauden ja yksityisyyden koetaan usein vaarantavan yhteiskunnan turvallisuuden, jos viranomaiset eivät voi aina halutessaan seurata ihmisten sähköistä viestintää. Samalla kuitenkin unohtuu, että vahvat kansalaisoikeudet kirjattiin Suomen perustuslakiin nimenomaan aikana, jolloin Suomessa oli vuosien ajan koettu poliittista väkivaltaa ja terrori-iskuja. 1800-1900 -lukujen taitteen poliittiset levottomuudet olivat saaneet kimmokkeensa nimenomaan kansalaisten perusoikeuksien kaventamisesta.

Turvallisuuden nojalla poliitikot ovat viime vuosina itse asiassa olleet pelottavan valmiita tinkimään sellaisista kansalaisten perusoikeuksista,

kuin sananvapaus ja yksityisyys. Pelon ja populismin ilmapiirissä kansalaisoikeuksista on tullut epäaihe, joka ei tunnu kiinnostavan ketään.

Sen sijaan poliitikot kilpailevat lähinnä siitä, kuka rajoittaisi kansalaisten oikeuksia eniten. Millaisia nettisuodattimia julkisten kirjastojen tietokoneisiin pitäisi asentaa, mitä sivuja tulisi blokata suomalaisten tietokoneiden ruuduilta ja mitä tietoja meidän elämästämme viranomaisten tulisi kerätä. Ja tällä on tietysti hyvä peruste, kuten terrorismi ja lapsiporno.

Suodatuslistalle haluttiin kuitenkin myöhemmin nettipokeria ja teletunnisteita vaadittiin annettavaksi myös tekijänoikeusjärjestöille. Kun suodattimet ja tietokannat kerran ovat olemassa, niitä on sen jälkeen helpompi myös käyttää.

Tai kuten eräs suomalainen ASEM-kokousedustaja kertoi Singaporen edustajan todenneen. ”Suodatattehan tekin lapsipornoa. Miksi me emme saisi estää kansalaisiamme näkemästä sopimattomia poliittisia mielipiteitä?”

Kansalaisoikeuksien sirpaleiset periaatteet

Suomessa tarvitaan kokonaisvaltaista poliittista keskustelua tietoyhteiskunnan kansalaisoikeuksista. Nyt debattia käydään yksittäisten lakien ympärillä, ilman kokonaiskuvaa.

Miksi esimerkiksi kaikkien puheluiden ja sähköpostien tunnistetiedot on tuoreen EU-direktiivin mukaan pakko kerätä poliisin ja turvallisuusviranomaisten mahdollisia rikostutkimuksia varten, mutta kirjepostin tunnistetietojen kerääminen on laitonta? Mikä on sähköpostin ja kirjepostin ratkaiseva ero? Esimerkiksi Yhdysvalloissa ei Unabomberin 18 vuotta kestäneen kirjepommikampanjan aikana tullut kenellekkään mieleen vaatia, että kaikkien kirjeiden ja postipakettien tunnistetiedot tulisi kerätä talteen siltä varalta, että jotain kirjettä käytettäisiin terroritekoon. Ei, vaikka pommit tappoivat kolme ja haavoittivat 29 ihmistä.

Kirjepostin tunnistetiedot sentään olisi mahdollista kerätä kattavasti. Sähköisessä tietoliikenteessä aukoton tunnistetietojen keruu on kuitenkin mahdotonta. Esimerkiksi tunnistetietojen keräämistä edellyttävä direktiivi koskee vain puheluiden, tekstiviestien, EMS-palveluiden (mitä ne sitten ovatkaan, EMS-palvelun käsitettä ei tunneta EU-asiakirjojen ulkopuolella), multimediapalveluiden, operaattoreiden sähköpostipalveluiden ja operaattoreiden nettipuhelupalveluiden tietoja. Sen sijaan esimerkiksi Skype-puheluista, pre paid -liittymistä soitetuista puheluis-

ta, yhteisötilaajien välittämistä sähköposteista, Gmailin ja Luukun kaltaisista nettisähköposteista, pikaviesteistä, chateistä, irc-keskusteluista, usenet-keskusteluista, freenet-viesteistä tai nettiselauksesta tietoja ei kerätä. Lisäksi viestit voi halutessaan myös piilottaa ja salata niin, että niiden jäljittäminen on teknisesti mahdotonta.

Vähänkin taitavampaa rikollista tai terroristia tunnistetietojen tallentaminen ei häiritse. Sen sijaan tavallisten kansalaisten tavallisesta tietoliikenteestä kerätään massiivinen tietokanta, jonka silkka olemassaolo on riski EU-kansalaisten yksityisyydelle. Esimerkiksi roskapostien lähettäjille ja identiteettivarkaille tietokannan sisältämät tiedot olisivat kultakaivos. Tiedot voivat päätyä vääriin käsiin myös vahingossa kuten Iso-Britanniassa kävi äskettäin, kun viranomaiset hukkasivat 25 miljoonan britin henkilötiedot.

Entä ulottuuko perinteinen luottamuksellisen viestin suoja, kirjesalaisuus myös sähköpostiin? Ei ilmeisesti työpaikoilla, koska työantajille halutaan antaa oikeus seurata työntekijöiden sähköpostiliikennettä mahdollisen liikesalaisuuksien vuotamisen selvittämiseksi. Sen sijaan kirjekuoreen sujautettu USB-muistitikku olisi edelleen luottamuksellinen viesti, jota työnantajalla ei olisi oikeutta lukea.

Tai miksi sananvapaus suojaa huumeiden valmistustekniikoista käytävää keskustelua, mutta kopiosuojausten kiertotekniikoita koskeva julkinen keskustelu on rikos?

Kuka valvoo valvojia?

Pelko ja populismi on vahva ja vaarallinen yhdistelmä, eikä demokratia suinkaan ole sille immuuni. Päinvastoin. Hyvänä esimerkkinä ovat J. Edgar Hooverin kommunistivainot Yhdysvalloissa. Mutta mitä Hooverin johtama FBI olisikaan saanut aikaan nykytekniikalla? Mitä olisi tapahtunut, kun se olisi voinut seurata kaikkien kaikkea tietoliikennettä ja valvoa meidän jokaista liikettämme?

Vallanpitäjät vaihtuvat ennemmin tai myöhemmin. Siksi hyväntahtoisellekaan hallitukselle ei edes tehokkuuden nimissä saa antaa välineitä, joilla voi liiaksi kontrolloida kansalaisten elämää. Ennemmin tai myöhemmin näitä välineitä käytetään myös väärin. Hollannin juutalaisten kohtalo natsien miehitettyä maan on tästä kaikista pelottavin esimerkki. Hollannin integroitu henkilötietojärjestelmä auttoi natseja tuhoamaan Hollannin juutalaiset nopeammin ja perusteellisemmin kuin missään länsimaissa.

Kyse on siitä, millaisten arvojen varaan me valvontateknologiat rakennamme. Internet on tunnettu esimerkki siitä, että teknologialla on

arvot. Sen perusprotokollat tunnetusti koodattiin Kalifornian kampuksella hippiliikkeen kultaisina vuosina - ”Information wants to be free”. Jokainen voi kuvitella, miltä Internet näyttäisi, jos ne perusprotokollat olisi koodattu Leningradin yliopiston kampuksella.

Sama pätee edelleen. Otetaan esimerkiksi varastettujen autojen etsiminen liikennevalvontakameroiden avulla, jota on esitetty. Tämähän on kannatettavalta kuulostava ajatus, vai mitä? Rekisterinumeroiden tunnistaminen valvontakameroiden kuvista onnistuu helposti. Mutta pitääkö ne kaikki kerätä tietokantaan, josta kaikkien autojen liikkeet on mahdollista selvittää kuukausia jälkikäteen. Ei ainakaan varastettujen autojen löytämiseksi. Siihen riittää aivan hyvin se tietokanta, jossa on varastettujen autojen rekisterikilpien numerot. Kerätään vain niiden liikkeet ja pystytään löytämään ne autot.

Haluammeko me tavalliset lainkuuliaiset kansalaiset, että viranomaisilla on tietokannoissaan tiedot meidän automme liikkeistä, meidän matkoistamme julkisissa liikennevälineissä, meidän puheluistamme ja meidän sähköposteistamme. Miten taataan näiden tietojen suoja väärinkäytöltä? Esimerkiksi siltä norjalaistoimittajalta, joka on jostain saanut käsiinsä tietoja viranomaisten ja pankkien tietokannoista. Tietoja vuotaneiden viranomaisten lahjonnastakin on puhuttu. Mutta täällä Suomessahan tämä ei ole mahdollista. Ei edes Sonerassa.

Kysymys siitä, kuka valvoo valvojia, on kysyttävä silloin, kun asiat ovat hyvin. Sillä siinä vaiheessa, kun viranomaiset käyttävät valvontavaltuuksia väärin, silloin on jo liian myöhäistä. Kysymyksen esittäminen voi olla mahdotonta tai ainakin vaarallista. Tai sitten kukaan ei enää pysty kuulemaan sitä kysymystä, kun viranomaisten nettisuodattimet estävät meitä näkemään sen.

Ovatko nämä perusteettomia kauhukuvia? Ei, vaan jokapäiväistä totta suurelle osalle maailman ihmisiä. Sitä paitsi suomalaiset yritykset ovat myös olleet kehittämässä näitä välineitä eri puolella maailmaa.

Turvallisuuden paradoksit

Me unohdamme helposti, että demokratiaa ei voi olla ilman vahvaa sananvapauden ja yksityisyyden suojaa. Että demokratiassa on oltava mahdollista elää ilman pelkoa, siis anonyymisti. Jos me päätämme tinkiä sananvapauden ja yksityisyyden periaatteista, lopputulos voi tuntua turvallisemmalta, mutta demokratiaa se ei enää ole. Eikä välttämättä turvallistakaan.

Yksityisyyden suojaaminen sellaisena, kuin se nykyään ymmärretään, voi osoittautua tietoyhteiskunnassa mahdottomaksi. Yritykset keräävät meistä tietoa tehdäkseen bisnestä ja viranomaiset palvellakseen meitä paremmin ja suojellakseen meitä rikollisuudelta. Yhä suurempi osa meidän liikkeistämme ja teoistamme tallentuu erilaisiin tieto- ja valvontajärjestelmiin.

Kenelläpä meistä voisi olla jotain sellaista salattavaa, jota emme soisi niin viranomaisten kuin kauppiaitten kuin vakuutusyhtiöiden kuin työtoverien kuin perheenjäsenten vapaasti urkkivan? Cyber Ark Software -yhtiön Englannissa äskettäin tekemässä selvityksessä kävi ilmi, että joka kolmas IT-osaston työntekijä oli joskus urkkinut työtovereidensa yksityisiä tietoja, esimerkiksi sähköposteja, dokumentteja ja palkkatietoja.

Helposti unohdetaan, että ihmisten tiedot ovat rahanarvoista tavaraa, ja niistä ovat naapureiden ja sukulaisten lisäksi kiinnostuneita myös rikolliset. Erilainen henkilötietojen väärinkäyttö ja suoranaiset identiteettivarkaudet yleistyvät maailmalla nopeasti.

Onko lainsäädännön tehtävänä suojella kansalaisia vallanpitäjiltä vai vallanpitäjiä kansalaisilta? Jos tätä kysymystä ei muista, niin käy helposti niin, ettei jäljellä ole kohta enää mitään suojelemisen arvoista. Kyse on siitä, millaista tietoyhteiskuntaa me olemme rakentamassa.

Tiedotusvälineissä keskustellaan usein tietomurroista ja viruksista, botneteistä ja palvelunestohyökkäyksistä. Meitä uhkaava vihollinen on aina kaukana – kansainvälinen rikollisliiga identiteettivarkaissa tai terroristijärjestö yhteiskuntaa rampauttamassa.

Cyber-Ark Software -yhtiön selvitys paljastaa kuitenkin, että se todellinen uhka piilee lähipiirissä. Jokainen voi kysyä myös itseltään mitä tekisi, jos käytössä olisi jäljittämätön pääsy esimerkiksi oman lapsen uuden poika- tai tyttöystävän sijainti-, ostos-, terveys-, pankki-, opiskelu- tai rikostietoihin. Kansalaisten tietoja sisältävät järjestelmät ja näiden tietojen käyttöprosessit onkin suunniteltava estämään paitsi ulkoiset hyökkäykset myös sisäiset väärinkäyttöyritykset.

Kansalaisjärjestöt ja ubiikkiyhteiskunta – kuuleeko kukaan?

Ville Oksanen

Villi ja vapaa Internet

Ei ole sattumaa, että sama maantieteellinen alue, joka synnytti hippiliikkeen, oli myös pitkälle Internetin ja koko nykyisen informaatioyhteiskunnan runkona toimivan teknologian kehityksen takana. San Franciscon alueen anarkistinen ja auktoriteetteja kunnioittamaton individualistinen ilmapiiri oli omiaan nostamaan pintaan ajatuksen ilman keskitettyä kontrollia toimivasta verkkoympäristöstä, jossa käyttäjät olisivat lähtökohtaisesti tasa-arvoisia.

Avoimuuteen perustuvan Internetin syntymä jäi pitkäksi aikaa pois niin yritysmaailman kuin yhteiskunnallisten päättäjien tutkaruuduilta. Käyttäjäkunta verkossa rajautui lähinnä akateemisten instituutioiden työntekijöihin. Tilanne oli onnekas, sillä se mahdollisti verkon rakentumisen kestämään jossain määrin paremmin vielä horisontin takana olleet poliittiset myrskyt, joiden tavoitteena oli kontrollin ja valvonnan lisääminen erilaisten yhteiskunnallisten tarkoitusperien nimissä.

Vielä 90-luvun alkupuolella ilmapiiri verkon vapauteen uskovien teknolibertaanisen ideologian kannattajien joukossa olikin hyvin toiveikas. Verkon hajautetun luonteen ja vahvojen kryptografisten metodien piti vapauttaa ihmiskunta kansallisvaltioiden holhouksesta. Tietynlaisena kulminaatiopisteenä voidaan pitää John Perry Barlowin kirjoittamaa Internetin itsenäisyysjulistusta ”A Declaration of the Independence of Cyberspace”:

> ..Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek

to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Valitettavasti tämä optimismi ei kestänyt pitkään. Kun kansallisvaltioiden viranomaiset ja poliittiset päättäjät huomasivat tämän uuden lähes kontrolloimattoman viestintä- ja informaationvälitysväylän olemassaolon, heidän ensimmäinen vaistonvarainen reaktionsa oli koettaa saada se mahdollisimman nopeasti perinteisen yhteiskunnallisen valvonnan piiriin.

Reaktio ei ollut täysin odottamaton. Radikaaleimmissa suunnitelmissa uuden Internetin myötä syntyvän maailmanjärjestyksen tunnuspiirteitä olisivat olleet mm. täydellinen sananvapaus (ei rajoituksia sisällön tai immateriaalioikeuksien suhteen), täydellisen luottamuksellinen kommunikaatio (poliisin ja turvallisuuspalveluiden mahdotonta valvoa kansalaisten viestintää) ja kokonaan anonyymit tili- ja maksujärjestelmät ilman verotusta. Nykyinen vastakkainasettelu verkon vapauden ja sen kontrolloimisen vaatijoiden välillä oli näin valmis.

Varsinkin Yhdysvalloissa kansalaisjärjestöt ovat näytelleet keskeistä roolia kansalaisten oikeuksien puolustamisessa verkkoympäristössä. John Barlowin ja John Gilmoren perustaman Electronic Frontier Foundationin lisäksi Electronic Privacy Center (EPIC) ja Center for Democracy and Technology ovat osallistuneet aktiivisesti poliittiseen keskusteluun ja kyenneet vaikuttamaan siihen. Silti todennäköisesti tuloksekkainta työtä on tehnyt Americal Civil Liberties Union, joka on ulottanut perinteisen perusoikeuksien valvontansa myös Internet-ympäristöön käyttäen hyväksi vuosikymmenien aikana kertynyttä tietotaitoaan.

Euroopassa vastaavaa kansalaisyhteiskunnan osallistumista ei juuri ole nähty muutamia yksittäisiä poikkeuksia lukuun ottamatta. Tässä kirjoituksessa syitä tilanteeseen etsitään lähtien liikkeelle artikkelin kirjoittajan kokemuksista Electronic Frontier Finland ry:n perustamisesta ja ”pyörittämisestä”.

Tätä subjektiivista lähestymistä täydennetään artikkelin toisessa osassa, jossa pohditaan, miksi kansalaisoikeudet ja erityisesti sananvapaus ja yksityisyys eivät ole politiikan agendalla korkealla. Artikkelin päättää synteesi siitä, mitä tilanne tarkoittaa ubiikkiyhteiskunnan kannalta.

EFFI verkkokäyttäjien edunvalvojaksi

Suomesta puuttui vielä 2000-luvulle siirryttäessä järjestö, joka olisi keskittynyt kansalaisoikeuksien puolustamiseen Internetissä. Suomalainen kriittinen tietoyhteiskuntakeskustelu olikin lähinnä yksittäisten henkilöiden kuten Risto Linturin ja Petteri Järvisen varassa. Asiaan päätettiin saada muutos – Berkeleyssä, n. 20 kilometriä San Franciscon pohjoispuolella.

Tämän artikkelin kirjoittaja ja Mikko Välimäki viettivät kesäkuun 2001 UC-Berkeleyn yliopiston SIMS-yksikössä (School of Information Management and Systems, nykyisin iSchool). Jossain vaiheessa puheeksi nousi kansalaisjärjestön perustaminen, joka toimisi kuten lahden toisella puolella San Franciscossa päämajaansa pitävä EFF (= Electronic Frontier Foundation). Halusimme käyttöömme äänitorven, jonka nimissä voisimme ottaa poliittisempia kantoja tutkimusteemoja sivuaviin aiheisiin. Kutsu perustamiskokoukseen saatiin lähtemään elokuun viimeisenä päivänä:

> *KUTSU ELECTRONIC FRONTIER FINLAND RY:N (EFFi) PERUSTAVAAN KOKOUKSEEN*
>
> Suomesta on puuttunut tähän asti järjestö, joka nostaisi julkisuuteen vailla sensaationhalua yksittäisiä Internetin käyttäjien ja ohjelmoijien yksityisyyttä ja sananvapautta uhkaavia ongelmia. EFFi ry perustetaan yhdysvaltalaisen esikuvansa Electronic Frontier Foundationin (http://www.eff.org/) päämääriä mukaillen täyttämään tämä aukko.
>
> Akateemisesta vapaudesta periytyville arvoille rakennettu Internet on yhä enenevässä määrin käyttäjien oikeuksia rajoittavien sääntelyhankkeiden kohteena. Perusteluina käytetään milloin kansallista turvallisuutta, milloin yrityselämän etuja. Useimmat näistä hankkeista ovat kuitenkin ylimitoitettuja tai jopa tuiki tarpeettomia. Hyvä esimerkki on uusi EU:n tekijänoikeusdirektiivi.
>
> Ulkomaisten esikuviensa mukaisesti EFFi rakennetaan järjestöksi, joka pystyy oikeasti vaikuttamaan lainsäädäntötoimintaan sen kaikilla tasoilla antamalla muun ohella lausuntoja lainsäädäntöhankkeista, järjestämällä koulutus- ja tiedotustilaisuuksia, sekä tarjoamalla oikeudellista neuvontaa.
>
> EFFi ry:n perustava kokous pidetään Hotelli Kämpin Paavo Nurmi-salissa keskiviikkona 5.9. alkaen klo 18:00.

Perustavassa kokouksessa kuullaan kirjailija Leena Krohnin ja professori Jukka Kemppisen alustukset aiheesta. Lisäksi kokouksessa päätetään toimintasuunnitelmasta ja valitaan EFFi ry:n hallitus. Osallistumisesta kiinnostuneita pyydetään ottamaan yhteyttä Ville Oksaseen.

EFFI:n toimintaa leimasi alusta alkaen aktiivinen tiedotuspolitiikka. Esimerkiksi jo perustamiskokouksesta lähetettiin lehdistötiedote STT:lle ja IT-lehdille. Ensimmäinen varsinainen lausunto käsitteli oikeusministeriön valmistelemaa sananvapauslakia ja se annettiin 15.9. - ennen kuin yhdistys oli edes saatu rekisteröidyksi yhdistysrekisteriin.

EFFI:n perustamisen lisäksi samaa konseptia yritettiin toteuttaa välittömästi myös EU-tasolla. EFFI:stä oltiin yhteydessä potentiaalisiin Eurooppalaisiin järjestöihin ja ehdotettiin yhteisen kattojärjestön perustamista. Eri järjestöjen väliset erot toiminnan tavoitteissa ja toimintamalleissa tekivät yhteistyön kuitenkin varsin hitaaksi ja tuskalliseksi.

Asiaa puitiin mm. Chaos Computer Conferenssin yhteydessä Berliinissä jouluna 2001 ja keväällä 2002 Bits of Freedomin järjestämässä seminaarissa Amsterdamissa. Lopputuloksena perustettiin Berliinissä 8.6.2002 European Digital Rights, joka suuntautuu lähinnä yksityisyyttä koskeviin kysymyksiin ja joka suhtautui varsin skeptisesti Electronic Frontier Foundationiin.

EFFI ja tekijänoikeuslain uudistaminen

Tekijänoikeuslain uudistaminen on ollut hanke, johon vaikuttamiseen EFFI:ssä on uhrattu selvästi eniten resursseja. Syitä priorisointiin on ollut kaksi. Ensinnäkin EFFI:n hallituksen jäsenet ovat olleet henkilökohtaisesti kiinnostuneet aihepiiristä. Toiseksi kyseessä on lainsäädäntö, jonka vaikutukset heijastuvat paljon laajemmalle kuin ”artistien työn korvaamiseen”. Esimerkiksi sääntely vaikuttaa suoraan sananvapauden ja yksityisyyden suojaan varsinkin verkkoympäristössä.

EFFI:n näkökulmasta hyvässä tekijänoikeuslaissa huomioitaisiin yhteiskunnan kokonaisetu. Nykyinen lainsäädäntö on kehitetty lähinnä eri eturyhmien (viihdeteollisuus, mediayhtiöt ym.) vaatimusten perusteella. Sen seurauksena laista on tullut spagettimainen kaaos yksittäisiin ongelmiin kohdistuvia pykäliä, joista on hyvin vaikea saada selvää. Keskeistä olisi myös, että lainsäädännöllä pyrittäisiin kannustamaan sitä tukevien sosiaalisten normien syntymistä nykyisen rangaistuksia korostavan linjan sijaan.

EFFI:n alkuvaiheen vaikuttaminen hankkeessa, ennen kuin laki ehti eduskuntaan, kohdistui erityisesti akateemisen salaustutkimuksen suojaamiseen. Tämä teema omaksuttiin suoraan USA:sta, jossa tutkijoita oli uhkailtu oikeustoimilla näiden paljastettua kopiosuojausten toiminnassa ilmenneitä merkittäviä puutteita. Teema oli myös siinä mielessä helppo valinta, ettei se ensinnäkään uhannut suoraan kenenkään muun eturyhmän etuja ja oli toiseksi helppo kehystää osaksi suomalaisen tietoturvateollisuuden kilpailukykyä.

Vaikuttamisessa käytettiin niin suoria yhteydenottoja OPM:n tekijänoikeusyksikköön kuin myös mm. yleisönosastokirjoituksia yliopistojen henkilökuntalehdissä. Toiminta oli tältä osin tuloksellista. Suomi on todennäköisesti ainoa maa Euroopassa, jossa salaustutkimus on nyt suojattu lain tasolla OPM:n lisättyä asiaa koskevan nimenomaisen pykälän lakiin.

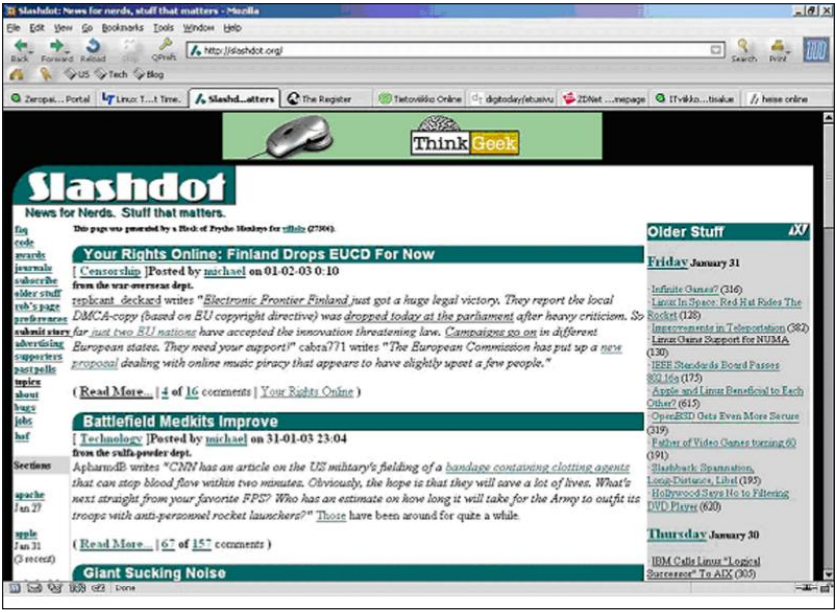
Alkumenestyksestä innostuneena EFFI laajensi tavoitteitaan, mutta kritiikin lisääntyessä Opetusministeriön into kuuntelemiseen laski merkittävästi. EFFI esimerkiksi poistettiin opetusministeriön lakia koskevalta tiedostuslistalta, koska kyseessä ei ollut ”virallinen järjestö”.

Tekijänoikeuslain ensimmäisen eduskuntakäsittelyn yhteydessä EFFI toimi kiinteässä yhteistyössä teknologiateollisuuden ja kirjastopuolen edustajien kanssa. Keskeisiä teemoja olivat teknisten suojauskeinojen rajaukset, ”kasettimaksun” jakokriteerit ja organisointi sekä teosten tuominen ETA-alueiden ulkopuolelta. Kuitenkin varsinainen päätavoite oli koko lakiesityksen kaataminen, koska sitä pidettiin liian monessa suhteessa ongelmallisena. Kaksi yhdistyksen edustajaa, allekirjoittanut ja Mikko Välimäki, pääsivät myös ajamaan asiaa sivistysvaliokunnan kuulemisissa:

> Hallituksen esitys on nykyisessä muodossaan liian ongelmallinen, jotta se kyettäisiin käsittelemään realistisesti ennen vaaleja ainakaan nykyisessä laajuudessaan. Erityisesti ehdotuksen teknisiä suojauksia koskeviin kohtiin tarvittaisiin merkittäviä muutoksia. Lisäksi ehdotuksessa on runsaasti yksittäisiä kohtia, jotka ovat joko direktiivin, perustuslain tai ihmisoikeussopimusten vastaisia ja jotka pitää joka tapauksessa korjata ennen lain hyväksyntää.
> *(Oksanen, 2003)*

Viesti meni tältä osin hyvin perille ja sivistysvaliokunta antoi lain poikkeuksellisesti raueta - tosin ratkaisevana tekijänä oli ehkä rehellisyyden nimissä perustuslakivaliokunnan ruuhkautuminen, mikä esti lausunnon saamisen ennen vaalilomalle siirtymistä. Laki siirtyi siis Vanhasen en-

simmäisen hallituksen valmisteltavaksi. EFFI tiedotti asiasta tapansa mukaan hyvin aktiivisesti ja lopputulos sai huomiota myös Suomen ulkopuolella.Sen sijaan varsinaista kansalaiskeskustelua ei syntynyt lain käsittelyn aikana käytännössä lainkaan.



Slashdot 01.02.2003

Opetusministeriön tekijänoikeusyksikkö käynnisti lainvalmistelun uudestaan. Tällä kertaa sen tueksi järjestettiin kolme kuulemista, joista teknisiä suojakeinoja koskeneeseen kuulemiseen EFFI osallistui aktiivisesti. Kuulemisilla ei juuri ollut vaikutusta lain sisältöön. Laki palasikin lähes muuttamattomassa muodossa eduskuntaan maaliskuussa 2004. Julkisuudessa laista nousi tässä vaiheessa esille lähinnä jumalanpalvelusmusiikin korvauskäytäntö, josta käytiin eri yleisönosastoilla väittelyä koko kevään 2004 ajan.

EFFI kutsuttiin tälläkin kertaa sivistysvaliokunnan kuultavaksi, mutta vastaanotto oli lähinnä muodollisen kohtelias. Asiaan saattoi vaikuttaa, että valiokunnan puheenjohtaja oli ollut kulttuuriministerinä valmistelemassa edellisen hylätyn esityksen opetusministeriön tekijänoikeusyksikön kanssa.

Yksikään EFFI:n valiokunnassa esittämä muutosesitys ei mennyt

läpi valiokunnan mietintöön, joka annettiin kevätistuntokauden lopulla. Kaiken lisäksi esitykseen oli lisätty viime hetkellä lakivaliokunnan toimesta täysin uudet pykälät, jotka asettivat täysin uusia velvollisuuksia Internet-operaattoreille – ilman yhtään kuulemista tai mahdollisuutta kommentoida muutoksia. Äänestys laista siirtyi kesälomien paluun jälkeiseen aikaan.

Lain toisessa pääistuntokäsittelyssä sivistysvaliokunnan esitys olisi mennyt muuten muuttamattomana läpi, mutta jumalanpalvelusmusiikkia koskeva kohta kääntyi äänestyksessä sivistysvaliokunnan esitykseen nähden päinvastaiseksi. Tämän seurauksena lakiesitys siirtyi suuren valiokunnan käsittelyyn. Ilman tätä muutosta esitys olisi hyväksytty ilman sen suurempaa kohua.

Jotain kuitenkin tapahtui. Mikrobitti oli tehnyt lain sisällöstä erittäin hälyttävän verkkoartikkelin, jota lainattiin laajalti eri blogeissa. Tuloksena oli Suomessa ennennäkemätön verkkoaktivismin aalto, jonka seurauksena mm. eduskunnan edessä nähtiin mielenosoitus, johon osallistui satoja lakiehdotusta vastustaneita kansalaisia.

Valitettavasti keskustelu takertui tällä kertaa käyttäjien oikeuteen siirtää musiikkia MP3-soittimiin ”kopiosuojatuilta” CD-levyiltä. EFFI koetti kiinnittää julkisuudessa huomiota esityksen muihin vakavampiin ongelmiin, mutta tällä ei ollut mitään vaikutusta.

Kulttuuriministeri Karpela epäili tätä viime hetken kritiikin aaltoa masinoiduksi toiminnaksi. Todellisuudessa kyse oli kuitenkin spontaanista reaktiosta. Tosin samalla kulisseissa oli käynnissä ankara viime hetken lobbaus, jolla pyrittiin saamaan erityisesti kokoomuksen kansanedustajia avaamaan koko lainsäädäntö suuressa valiokunnassa. Sääntöjen mukaan tämä olisi ollut teoriassa mahdollista.

Hanke olisi ehkä voinut onnistua, mutta ministeri Karpelan tehtyä asiasta henkilökohtaisen arvovaltakysymyksen, hallituksen edustajat palasivat ankarasta julkisesta paineesta huolimatta ruotuun ja tukivat esitystä. Suuri valiokunta hyväksyikin lopulta lain lähes hampaattoman ponnen kera ja eduskunnan istuntokäsittelyssä ei asiaan enää sen kummemmin puututtu.

Yhteenvetona EFFI:n vaikutus jäi loppujen lopuksi varsin pieneksi ja Suomeen tuli merkittävästi direktiiviä tiukempi tekijänoikeuslaki. Konkreettisesti EFFI sai tavoitteistaan läpi ainoastaan kaksi muutosta eli edellä mainitun tutkijoita suojaavaan pykälän sekä - direktiiviin vastaisen - teknisten suojausten dekompilaatiokiellon poiston, jossa kyse oli lähinnä teknisestä muutoksesta. Toisaalta EFFI:n kritiikki saattoi

osalta vaikuttaa siihen, ettei laista tullut vieläkin enemmän oikeudenhaltijoita suosiva.

Ehkä katkerinta EFFI:n näkökulmasta on se täydellinen kuurous, jolla eduskunta suhtautui järjestön puhtaan teknisiin korjausehdotuksiin toisen käsittelyn yhteydessä. Mahdollisesti syynä tähän oli kansanedustajiin aktiivisesti ja ammattitaitoisesti istutettu näkemys EFFI:stä lähinnä yhden asian (ts. verkkopiratismin edistävänä) liikkeenä?

EFFI ja ohjelmistopatentit

Toinen EFFI:n toimintaan keskeisenä kuulunut teema on ohjelmistopatenttien vastustaminen. EFFI:n näkökulmasta ohjelmistopatentit eivät sovellu ohjelmistotuotantoon, koska niiden avulla on mahdollista rajoittaa tarpeettoman paljon kilpailua jo ennestään monopolisoitumiselle herkällä toimialalla.

Ongelmistaan huolimatta tekijänoikeuslaki tarjoaakin riittävän suojan innovatiivisen ohjelmistosektorin olemassaololle. Päinvastoin kuin tekijänoikeuslain yhteydessä, ohjelmistopatenttien yhteydessä järjestö oli mukana ajoissa ja pääsi näin vaikuttamaan suoraan direktiivin valmisteluun.

Vaikuttamisessa käytettiin ns. monikärkistrategiaa (vrt. Pugatch 2004, The International Political Economy of Intellectual Property Rights) eli tavoitteena oli lähestyä kaikkia prosessiin osallistuvia viranomaistahoja. EFFI:stä oltiinkin aktiivisesti yhteydessä niin asiaa valmistelleisiin virkamiehiin, asiaa eduskunnassa käsitelleisiin kansanedustajiin kuin myös eurokansanedustajiin. Tämän lisäksi erityistä vaivaa nähtiin ruohonjuuritason kampanjoinnin aktivoimiseksi mm. käynnistämällä asiaa koskeva netti-addressi.

Konkreettisella tasolla EFFI:n tavoitteena oli saada Suomelle ohjelmistopatenteista kielteinen kanta ministerineuvostoon ja saada mahdollisimman moni eurokansanedustaja äänestämään sen mukaisesti. Patentoinnille myönteisen pohjaesityksen kirjoittaneeseen komissioon ei pyritty edes vaikuttamaan.

Ongelmallisinta ohjelmistopatenttien vastaisessa vaikuttamisessa oli asian hyvin tekninen luonne. Ensinnäkin tietokoneohjelman ja saman asian toteuttavan sähkömekaanisen ratkaisun välinen ero on veteen piirretty viiva. Toiseksi käsitys tietokoneohjelmista ja niiden tuotantoprosesseista ei kuulu keskivertopoliitikon yleissivistykseen. Kaiken lisäksi asiaa kuvaava patenttilainsäädäntö ja erityisesti sen tulkintakäytäntö on äärimmäisen epäselvää – Euroopan patenttiviraston asiaa koskevat lin-

jaukset ovat mm. ristiriidassa keskenään. Tämän seurauksena huomattavan suuri osa ajasta meni ns. ”rautalangan vääntämiseen” eli selventämiseen siitä, mistä asiassa oli oikein kyse.

Asiaa ei helpottanut, että ohjelmistopatentoinnin puolustajat käyttivät sumeilematta tilannetta hyväkseen ja yrittivät hämärtää entisestään käytyä keskustelua. Erityisen suosittuna teemana oli antaa ymmärtää, että direktiivi ei muuttaisi mitään, vaan kirjoittaisi vain auki jo käytössä olevan Euroopan patenttiviraston tulkintakäytännön. Kaikki muutokset direktiiviin horjuttaisivat näin olemassa olevia kilpailuasetelmia EU:ssa.

Patentoinnin puolustajilla, joihin kuuluivat käytännössä kaikki isoimmat ICT-yritykset (Nokia, Siemens, Phillips jne), yritysten edusvalvontajärjestöt kuten EICTA ja UNICE, patenttiasiamiehet järjestöineen sekä tietyt USA:laiset toimijat kuten Chamber of Commerce, oli hallussaan täydellinen resurssiylivoima.

Patentointia vastustivat lähinnä avointa lähdekoodia kannattavat yksittäiset henkilöt ja muutamat PK-yritykset, kuten norjalainen Trolltech ja suomalais-ruotsalainen MySQL. Vastustajilla oli kuitenkin suhteellisen hyvin toimiva eurooppalainen kattojärjestö FFII, joka pystyi koordinoimaan niin varsinaista lobbausta kuin myös siihen kiinteästi liittyvää rahankeruuta yms.

Varsinainen prosessi on liian monipolvinen kuvattavaksi tässä. EU-tason tapahtumista on kuitenkin julkaistu yksityiskohtainen Florian Muellirin kirjoittama kuvaus ”No Lobbyists As Such - The War over Software Patents in the European Union”.

Valitettavasti kirjassa ei noteerata EFFI:ä, joka kuitenkin osallistui toimintaan aktiivisesti myös EU-tasolla. Järjestön edustajat olivat lobbaamassa parlamentissa ennen molempia äänestyksiä. Tämän lisäksi järjestön edustajat osallistuivat mm. FFII:n asiaa koskeneeseen seminaariin Brysselissä.

Suomessa ainoana ”liikkuvana” palasena oli eduskunnan talousvaliokunta, joka linjasi lopullisesti Suomen virallisen kannan asiaan. KTM:n virkamiehet olivat käytännössä alusta alkaen patentoinnin kannalla. Tästä huolimatta he kohtelivat EFFI:ä hyvin kohteliaasti. Järjestö mm. kutsuttiin kertaalleen yhdessä Nokian kanssa yksityiseen kuulemistilaisuuteen tilanteen muututtua kriittiseksi EU:ssa.

EFFI oli myös kutsuttuna talousvaliokunnassa, jonka lisäksi järjestö teki kiinteää yhteistyötä valiokunnan jäseninä olleiden selkeästi ohjelmistopatentoinnin vastaisten kansanedustajien kanssa (lähinnä Sari Essayah ja Merikukka Forsius).

EFFI:n strategiana oli pitää asia mahdollisimman selväpiirteisenä ja välttää väittelyä yksittäisten pykälien sisällöstä. Tätä varten kehitettiin mm. seuraava yksinkertainen testi hyväksyttävällä direktiiville:

> ”EFFI:n näkemyksen mukaan Suomen tulisi tukea linjaa, jossa tietokoneohjelmat voivat edelleen olla osa keksintöä, mutta jossa keksinnöltä edellytetään myös fyysistä elementtiä, joka ei voi olla pelkkä yleisluontoinen tietokone. Yksinkertaisena testinä EFFI:n mielestä onnistuneelle direktiiville ovat seuraavat kolme kysymystä, joihin pitäisi voida vastata kielteisesti:
>
> 1. Voidaanko henkilö, joka on kirjoittanut tekstinkäsittelyohjelman ja joka jakaa sitä kotisivullaan, haastaa oikeuteen välillisestä tai välittömästä patenttirikkomuksesta?
> 2. Voidaanko Linux-käyttöjärjestelmää jakeleva yritys haastaa oikeuteen välillisestä tai välittömästä patenttiloukkauksesta?
> 3. Onko matkapuhelimien tukiaseman toimintaa kontrolloivan kokonaisuuden patentointi mahdotonta?”[1]

Muuten valiokuntakuuleminen meni odotettuja ratoja. KTM:n jatkolausunnoin sanoin:

> ”Lausunnonantajista Teollisuuden ja työnantajain keskusliitto, Nokia, Teknologian kehittämiskeskus (TEKES) sekä Patentti- ja rekisterihallitus ovat pääosin tukeneet valtioneuvoston esittämää kantaa. Vastakkaista näkemystä ovat edustaneet Electronic Frontier Finland (EFFI ry), SOT Oy Ohjelmistoyhtiöt sekä europarlamentaarikko Piia-Noora Kauppi.”

Lopputuloksen ratkaisi käytännössä Nokian Ilkka Rahnasto, joka kutsuttiin hätiin ylimääräiseen kuulemiseen valiokunnan kannan näyttäessä muodostuvan patentoinnin vastaiseksi. Hän pääsi käyttämään useamman tunnin kansanedustajien kanssa ilman, että kukaan olisi päässyt kyseenalaistamaan hänen esittämiään väitteitä. Rahnaston tueksi KTM:lta pyydettiin lisäksi jatkolausunto, jossa pyrittiin kumoamaan valiokunnassa esitettyä kritiikkiä. EFFI ehti vielä toimittaa konkreettisesti yhdessä yössä oman vastineensa jatkolausuntoon, mutta todennäköisesti sitä ei enää valiokunnassa juuri lu-

---

[1] Mielenkiitoisesti KTM reagoi EFFI:n testiin jatkolausunnossaan (mainitsematta sitä nimeltä): ”...Todennäköisyys tahattomaan patentinloukkaukseen ei esitetyissä tapauksissa ole kuitenkaan sen suurempi tai pienempi kuin millään muullakaan tekniikan alalla. Esitettyjen kolmen kysymyksen ei siten voida katsoa toimivan yksikertaisena testinä onnistuneelle direktiiville”

ettu. Valiokunta hyväksyikin valtioneuvoston esityksen – tosin Merikukka Forsiuksen eriävällä mielipiteellä varustettuna.

EU:n parlamentissa lopputulos oli sitten toinen. Parlamentti kaatoi koko direktiivin toisessa käsittelyssä ja suomalaisista eurokansanedustajista enemmistö äänesti kaatamisen puolesta.

EFFI ja Enforcement-direktiivit

EFFI on kampanjoinut aktiivisesti myös ns. Enforcement-direktiivejä vastaan. Kyseisillä direktiiveillä on pyritty harmonisoimaan oikeudenhaltijoiden käytössä olevat oikeusturvakeinot kaikkien immateriaalioikeuslajien osalta. Kyseessä on ollut siis jälleen kerran ”one size fits all” -lähestymisestä, mikä johtaa väistämättä ei-optimaaliseen lainsäädäntöön. EFFI:n näkökulmasta suurin ongelma direktiiveissä oli kuitenkin, että oikeudenhaltijat ja komissio tekivät kaikkensa vesittääkseen niissä kaupallisen tuotepiratismin ja tavallisten kansalaisten mahdollisesti lainvastaisen toiminnan eron.

Ensimmäinen direktiivi koski (lähinnä) siviilioikeudellisia oikeusturvakeinoja ja toisen, vielä käsittelyssä olevan direktiivin (ja sitä tukevan puitepäätöksen) tavoitteena on säännellä rikosoikeudellisia sanktioita.

Ensimmäisen direktiivin käsittelyn yhteydessä EFFI:n toiminta rajoittui kirjallisen lausunnon toimittamiseen lakivaliokunnalle, jossa toivottiin ensisijaisesti Suomen neuvottelutavoitteen olevan direktiivin palauttaminen valmisteluun komissioon ja toissijaisesti:

”1. Direktiivin ulottuvuuden rajaaminen tuoteväärennöstapauksiin.
2. Direktiivin merkittävästi selvempi alisteisuus kilpailuoikeudelle.
3. Oikeudenhaltijoiden yksipuolisten tiedonsaantioikeuksien merkittävä rajaaminen nykyisestä ja yksityishenkilöiden oikeusturvan parantaminen prosesseissa.
4. Nykyisen oikeustilan säilyttäminen verkkopalvelujen tarjoajien vastuiden ja velvollisuuksien kohdalla.
5. Direktiivin seuraamislistan sisällön järkeistäminen esim. takavarikoiden ja tuotteiden takaisinkutsumisen kohdalla.
6. Teknisiä suojauskeinoja koskevan kohdan poistaminen.”

Lakivaliokunta hyväksyi kuitenkin hallituksen kannan sellaisenaan. EFFI:n näkökulmasta ehkä isoin ongelma oli, että Suomen lainsäädäntö

oli jo valmiiksi pitkälle ehdotetun direktiivin mukainen, joten se ei olisi tosiasiallisesti tarkoittanut kovin suurta muutosta.

EFFI:n edustaja (eli tämän artikkelin kirjoittaja) oli paikalla myös Strasbourgissa, kun asiaa käsiteltiin EU-parlamentissa. EFFI:n jäseniä kannustettiin myös ottamaan aktiivisesti yhteyttä MEP:hin. Lopputulos ei ollut huono, sillä enemmistö suomalaisista edustajista äänesti loppujen lopuksi EFFI:n (ja FFII:n) äänestyssuosituksen mukaisesti huolimatta siitä, että parlamentin isot ryhmät olivat direktiivin takana. Direktiivi kuitenkin hyväksyttiin pienin muutoksin ministerineuvoston ja parlamentin välisten epävirallisten neuvotteluiden jälkeen.

Direktiivin kotimaisen implementoinnin yhteydessä EFFI kutsuttiin kuultavaksi lakivaliokuntaan. Kuten edellä mainittiin, direktiivistä ei seurannut merkittäviä muutospaineita Suomelle. Sen sijaan EFFI koettikin käyttää tilaisuutta hyväksi ja vaatia valiokunnassa korjauksia tekijänoikeuslakiin jääneisiin virheisiin. Yritys ei saanut osakseen kuitenkaan mitään vastakaikua ja tuntuikin vahvasti, että Lex Karpelan yhteydessä hetkellisesti herännyt poliittinen kiinnostus aihepiiriin oli haihtunut ilmaan.

Muutenkaan EFFI:n kommenteista ei jäänyt juuri mitään jälkeä valiokunnan kannanottoon. EFFI:n keskeisin vaatimus oli, että uutena siviilioikeudellisena sanktiona lakeihin lisättävä oikeudenkäynnin tuloksen julkaiseminen vastaajan kustannuksella olisi rajattu A) ainoastaan kaupalliseen toimintaan tai B) ainakin mahdollistettu sekä kantajalle että vastaajalle. Valiokunnan puheenjohtaja Tuija Brax tuntui valiokuntakäsittelyssä ymmärtävän, miksi pykälän ehdotettu asymmetria sopisi hyvin huonosti siviilioikeudelliseen prosessiin, mutta syystä tai toisesta tämä ei kuitenkaan näkynyt valiokunnan lausunnossa.

Ensimmäisen direktiivin käsittelystä viisastuneena EFFI teki kotiläksynsä huolellisemmin toisen direktiivin kohdalla. Tilannetta helpotti myös se seikka, että Suomen virallinen kanta oli valmiiksi varsin skeptinen EU:n toimivaltaan harmonisoida rikosoikeudellisia sanktioita. EFFI tapasi mm. etukäteen kokoomuksen eduskuntaryhmän asian käsittelyyn osallistuvia kansanedustajia ja lähestyi muiden puolueiden edustajia lähinnä sähköisesti.

EFFI:n oli toisen direktiivin yhteydessä myös helpompi muodostaa yksiselitteisen ytimekäs kanta asiaan:

> ”EU:ta on arvosteltu aivan liian aktiivisesta direktiivitehtailusta. Nyt käsittelyssä oleva ehdotus on tyyppiesimerkki tästä. Sen hyödyllisyys, järkevyys ja oikeusperusta ja sisältö voidaan kyseenalaistaa - kuten hallitus tekee normaalia kriittisemmässä

kannanotossaan. Yksi askel jää kuitenkin hallituksen kannasta puuttumaan. Näkemyksemme mukaan se tulisi kuitenkin ottaa: EFFI:n mielestä Suomen virallisen kannan tulisi olla, että ehdotus hylätään.”

EFFI (jota tämän artikkelin kirjoittaja edusti) oli kutsuttuna talousvaliokunnan kuultavaksi yhdessä hovioikeudenneuvos Antti Miettisen (Suomen teollisoikeudellinen yhdistys ry) ja pääsihteeri Marja-Leena Mansalan (IPR University Center) kanssa. Tällä kertaa valiokunta sai kuulla asiantuntijoilta käytännössä yksimielisen tyrmäyksen direktiiville – viestinä oli, että edes oikeudenhaltijat eivät kaivanneet direktiiviä. Tästä huolimatta valiokunnan lausunnossa ei oltu valmiita muuttamaan hallituksen kriittisen hyväksyvää kantaa puhtaan kielteiseksi.

Lausuntoon jätettiin kuitenkin poikkeuksellisen voimakkaasti tylysanainen mielipide, jonka takana oli puolet valiokunnan käsittelyyn osallistuneista edustajista (Sari Essayah (kd), Martin Saarikangas (kok), Martti Korhonen (vas), Jere Lahti (kok), Jouko Laxell (kok), Juhani Sjöblom (kok) ja Oras Tynkkynen (vihr)):

> Valiokunnan lausunnossa on tuotu esille teollis- ja tekijänoikeuksien tehokkaan suojan lähtökohtainen tärkeys yhteisön innovaatiotoiminnan kannalta. Samalla on kuitenkin kiinnitetty huomiota esityksen valmistelun vakaviin puutteisiin, kyseenalaistettu rikosoikeudellisten menettelyjen tarkoituksenmukaisuus ja harmonisointitarve sekä kiinnitetty huomiota oikeudenhaltijoiden kannalta ylimitoitettuun sääntelyyn ja epäselvään soveltamisalaan teollis- ja tekijänoikeusrikoksissa.
>
> Asiantuntijalausunnoissa tuotiin lisäksi esille, että direktiivin ja puitepäätöksen implementointi merkitsisi aivan uudenlaisen systemoinnin ja rikosoikeudellisen ajattelutavan ja seuraamusjärjestelmän kehittämistä yksinomaan teollis- ja tekijänoikeudellisiin rikoksiin, ja nähtiin ongelmallisena sen synkronoiminen muuhun rikoslakiin.
>
> Edellä mainittujen seikkojen lisäksi lähes kaikissa asiantuntijalausunnoissa oli kiinnitetty huomiota sääntelyn oikeusperustaan ja kyseenalaistettu sen kuuluminen ylipäätään yhteisösääntelyn piiriin...Euroopan unionilla ei ole toimivaltaa luoda itselleen uusia valtuuksia, vaan valta unionin perustana olevien sopimusten muuttamiseen on jäsenmailla.
>
> ...

Edellä olevan perusteella ehdotamme, että valiokunta esittää kantanaan, että valtioneuvosto ei puolla direktiivin ja puitepäätöksen hyväksymistä.

Direktiivin kohtalo on toistaiseksi auki – parlamentti on äänestänyt sen puolesta ja asia menee seuraavaksi ensimmäiseen ministerineuvoston käsittelyyn.

Sähköinen sananvapaus ja teletietojen tallennusvelvollisuus

EFFI on ollut toki mukana myös monissa muissa lainsäädäntöprosesseissa kuin edellä mainituissa kolmessa tapauksessa. Ehkä menestyksekkäin oli järjestön alkuvaiheeseen osunut kampanjointi ”sähköisen sananvapauden vastuulain” järkevöittämiseksi, missä järjestön edustaja, tohtori Kai Puolamäki oli jopa kuultavana asiantuntijana perustuslakivaliokunnassa.

EFFI onnistui yhdessä teleoperaattoreiden kanssa mm. rajaamaan merkittävästi lakiin suunniteltua tallennusvelvollisuutta julkaisuille sekä järkevöittämään merkittävästi verkkojulkaisun määritelmää. Sen sijaan lakiin jäänyt poikkeuksellisen laaja lähdesuoja, joka koskee myös blogeja, oli puhdas lainsäädäntötekninen onnekas sattuma, josta EFFI ei valitettavasti voi ottaa kunniaa.

Tätä tekstiä kirjoittaessa taistelu teletietojen tallennusvelvollisuudesta on myös saavuttamassa loppuhuipentumansa. EFFI on panostanut paljon töitä tämän länsimaisen syyttömyysolettamuksen kumoavan hankkeen pysäyttämiseksi eli esimerkiksi järjestänyt kolme seminaaria ja yhden kansalaisvetoomuksen aihepiiristä.

Asian valmistelusta vastannut liikenne- ja viestintäministeriö on tehnyt EFFI:n näkökulmasta sinänsä hyvää työtä varsinkin EU-tasolla direktiivin sisällön rajoittamiseksi niin, että kaikkea Internet-liikennettä ei tarvitse tallentaa, kuten alkuperäiset ehdotukset olisivat edellyttäneet.[2] Kuitenkin direktiivi velvoittaa nykymuodossaankin huomattavan laajaan tietojen tallentamiseen ja esimerkiksi matkapuhelinliikenteestä tulee tallentaa puhelujen ajankohdat, tiedot kenelle on soitettu (myös vastaamattomien puhelujen osalta) sekä puhelimen sijaintitiedot. Näiden tietojen avulla ihmisen liikkuminen kyetään jäljittämään huomattavalla tarkkuudella kuten myös kuuluminen erilaisiin sosiaalisiin verkostoihin.

---

[2] Toisaalta kyynisesti voisi ajatella, että alkuperäiset kaikista laajimmat esitykset olisivat olleet ehkä jopa ”parempia” EFFI:lle, koska niiden kohdalla olisi ollut helpompi perustella, miksi kyse on oikeasti peruuttamattomasta ja erittäin kalliista isovelivaltion rakentamisesta.

EFFI:n toiminta ei toki ole myöskään rajoittanut pelkästään lainsäädäntöhankkeiden kritisointiin. Järjestö on osallistunut esimerkiksi aktiivisesti kopiosuojausten vastaiseen kampanjointiin julkaisemalla tietoja kopiosuojatuista levyistä ja niihin liittyvistä ongelmista.

Järjestön strategisesti juuri ennen joulusesonkia 2002 julkaisema ”EFFI varoittaa ostamasta ”CD-levyjä” pukinkonttiin” sai harvinaisen voimakkaan vastustuksen musiikkiteollisuudelta, joka ei tuolloin vielä uskonut, ettei CD-levyihin voi rakentaa järkevää kopiosuojausta jälkikäteen. Sittemmin EFFI:n kanta on osoittautunut oikeaksi ja tällä hetkellä CD-levyissä ei enää yritetä käyttää kopiointia haittaavia ”virityksiä”. Samoin musiikin verkkojakelussa trendi on hyvin vahvasti suojaamattoman musiikin jakelun lisäämisessä EMI:n ja Universalin päätettyä luopua ainakin väliaikaisesti kopiosuojauksista.

EFFI:n harjoittama kansalaisoikeuksien puolustaminen verkossa ja räväkät kommentoinnit ovat tuoneet järjestölle myös vastustusta. Järjestön edustajia on uhattu ja sen toimista on jätetty tutkintapyyntöjä.

Poliittisen toiminnan mallit

EFFI:n toiminnassa päätöksentekoon vaikuttaminen on tapahtunut hyvin konkreettisesti – tietyn lausunnon tai lehdistötiedotteen seurauksena jotain on tapahtunut tai useimmiten valitettavasti ei ole tapahtunut. Asiaa voidaan kuitenkin lähestyä myös teoreettisemmin.

Poliittisiin päätöksentekijöihin vaikuttavat samat lainalaisuudet kuin muihinkin valintatilanteisiin joutuviin henkilöihin. Aluetta on tutkittu runsaasti erityisesti psykologiassa ja kognitiotieteissä, mutta myös taloustieteen puolelta löytyy välineitä (erityisesti ”Public Choice Theory”), joilla lopputuloksia voidaan ainakin jossain määrin selittää.

Taloustieteellisestä näkökulmasta poliitikko tai virkamies voi pyrkiä ensisijaisesti maksimoimaan oman etunsa, mikä voi tarkoittaa esimerkiksi valtaa ja resursseja tai uudelleenvalintamahdollisuuksia. Yleinen etu on tähän verrattuna toisarvoista, mutta luonnollisesti yksi tekijöistä, jotka ovat pakko ottaa laskelmissa huomioon.

Alueen kilpaillusta luonteesta johtuen heikoimmat toimijat tippuvat pelistä aivan vastaavasti kuin ”perinteisemmillä” markkinoilla. Mukana pelissä ei kuitenkaan ole ainoastaan päätöksentekijät vaan myös muut intressitahot, joihin päätöksillä voisi olla negatiivisia tai positiivisia vaikutuksia – puhutaan ns. public rent seeking -ilmiöstä (julkistaloudellinen lisäarvon tavoittelu).

Konkreettisena esimerkkinä tästä levy-yhtiöiden kannattaa todennä-

köisesti investoida rahaa lobbaamiseen, jotta tekijänoikeuden kestoa pidennettäisiin tuottajan oikeuden osalta. Sijoitetulle rahalle saadaan mahdollisesti hyväkin tuotto pidentyneiden monopolivoittojen muodossa. Vastaavasti kansalaisten kannattaisi sijoittaa pidentämisen vastaiseen lobbaukseen, mutta tässä kohtaa tulee ongelmaksi vapaamatkustaminen ja yksittäisen kansalaisen hyvin pieni taloudellinen intressi, mikä tekee toiminnan koordinoimisen lähes mahdottomaksi.

Perinteisempi taloustiede olettaa, että ihmiset toimivat rationaalisesti. Tämä on kuitenkin vain rajoitetusti totta, koska ihmiset eivät kykene hahmottamaan yleensä kovinkaan täsmällisesti päätöksentekoon vaikuttavia tekijöitä ja niiden vuorovaikutussuhteita. Erityisen totta tämä on riskien kohdalla, joissa riskien luonteesta riippuva yli- tai aliarvostaminen on sääntö, ei poikkeus. Schneiner on koonnut seuraavan taulukon, josta käy hyvin ilmi ilmiön luonne:

Riski yliarvioidaan	Riski aliarvioidaan
Poikkeuksellisen vaikuttava	Tavanomainen
Harvinainen	Yleinen
Henkilöön sidottu	Anonyymi
Ei omassa vaikutuspiirissä	Omassa vaikutuspiirissä
Paljon puhuttu	Vähän puhuttu
Ihmisen aiheuttama	Luonnollinen
Välitön	Myöhemmin tapahtuva
Yhtäkkinen	Epämääräisenä hetkenä tapahtuva
Vaikuttaa henkilökohtaisesti	Vaikuttaa muihin
Uusi ja tuntematon	Hyvin tunnettu
Kohdistuu lapsiin	Kohdistuu aikuisiin
Moraalisesti arveluttava	Moraalin sallima
Ilman välillishyötyjä	Osittain hyödyllinen
Poikkeaa nykytilasta	Nykytilan mukainen
Bruce Schneider, The Psychology of Security (2007)	

Ihmiset tekevät myös muita säännönmukaisia ”virheitä”. Esimerkiksi testeissä on havaittu, että väitetyn nykytilan muuttaminen vaatii aina paljon paremmat perustelut kuin sen säilyttäminen – vaikka todellisuudessa kyse olisikin aivan samasta asiasta vain eri tavalla kehystettynä. Samoin vaihtoehtojen määrä vaikuttaa lopputulokseen – ihmiset valitsevat mielellään keskiarvon mukaisen vaihtoehdon eikä ylintä tai alinta vaihtoehtoa.

Kokonaan oma lukunsa (tai kirjansa, esim. Cass Sunnstein, Infotopia: How Many Minds Produce Knowledge, 2006) olisi ryhmätilanteisiin liittyvät päätöksenteon ongelmat. Ryhmät esimerkiksi usein päätyvät radikaalimpaan lopputulokseen, mikä olisi ollut kenenkään yksittäisen osallistujan mielipide.

Ryhmissä oikeaa informaatiota ei välttämättä oteta huomioon, jos se tulee vääräksi koetulta taholta. Vastaavasti asiantuntijaksi koetulta henkilöltä ollaan valmiita hyväksymään faktoja, jotka normaalisti tiedostettaisiin välittömästi vääräksi. Tosin usein henkilöt eivät edes halua tuoda oikeaksi tietämäänsä informaatiota ryhmän käyttöön, jos se voisi vaarantaa heidän asemansa yhteisössä.

Toisin sanoen, jos poliitikko haluaa säilyä virassaan, hänen kannattaa huomioida äänestäjäkuntansa mielipiteet. Koska äänestäjät pelkäävät eniten harvinaisia, näyttäviä ja heille vieraita riskejä (”lööppiriskit”), näihin kohdistetuilla toimenpiteillä saavutetaan paras ”tuotto” poliitikon kannalta – vaikka kansantaloudellisesti olisikin usein paljon järkevämpää puuttua yleisiin ja pieniin riskitekijöihin.

Tämä voisi selittää, miksi esimerkiksi terrorismin vastaiseen taisteluun käytetään miljardeja, vaikka tavallisen ihmisen riski kuolla terroristihyökkäyksessä on todella marginaalinen ja vaikka samoilla resursseilla voitaisiin saada paljon parempia tuloksia esimerkiksi lisäämällä syöpien seulontatutkimuksia. Sama logiikka toimii myös virkamiesten puolella. Esimerkiksi moottoripyöräjengit, huumekauppiaat tai pedofiilit tarjoavat hyvän uhkakuvan, joiden varjolla voidaan myydä muita intressejä ja hankkeita, kuten on jo monta kertaa nähty esimerkiksi Internetin valvontaa koskevan keskustelun kohdalla.

Kansalaisjärjestön mahdollisuudet

EFFI:n kaltaisille kansalaisjärjestöille viesti edellä mainitusta on selvä ja synkkä. On turha koettaa argumentoida esimerkiksi sananvapauden hitaan kapenemisen aiheuttamista riskeistä, koska se ei ole poliittisen järjestelmän kannalta ”myyvä” aihe. Koska sen vaikutukset eivät myöskään välttämättä heti näy, voidaan kuvitella nykytilan jatkuvan. Sen sijaan tarvitaan radikaaleja ja näkyviä yksittäistapauksia (”päiväkodin lapset joutuvat maksamaan tekijänoikeusmaksuja”) ja keinoja personoida riskit (”et voi jatkossa siirtää musiikkia MP3-soittimellesi”), jotka iskevät tavallisten kansalaisten arkeen.

EFFI:n tähänastiset kokemukset poliittisesta päätöksenteosta tukevat pitkälle edellä esitettyä analyysiä. EFFI:n ajamat asiat ovat koettu vie-

raiksi ja järjestön asiantuntemukseen ei ole luotettu pääsääntöisesti edes niissä tapauksissa, jossa kyse on ollut jokseenkin ilmeisten virheiden osoittamisesta, koska informaation tuoja on ollut ”väärä”.

Muutoksia on tapahtunut vain niissä tapauksissa, joissa EFFI:n edustaja on koettu oikeaksi asiantuntijaksi alueesta, kuten Kai Puolamäen esiintyessä perustuslakivaliokunnassa. Osittain järjestö saa syyttää lopputuloksesta myös itseään, koska se ei ole kyennyt aktivoimaan äänestäjiä ja markkinoimaan asioita heille siten, että niistä olisi syntynyt kiinnostusta. Järjestön esittämät uhkakuvat ovat olleet liian kaukana ihmisten arjesta tai poikenneet liikaa ”Status Quo”:sta ollakseen hyväksyttäviä.

Kansalaisvaikuttaminen ja ubiikkiyhteiskunta

Ubiikkiyhteiskunnan myötä IT-järjestelmiin lisääntyvät riskit tulevat väistämättä vielä lisääntymään nykyisestä. Tietoteknologian ja verkon ote kansalaisista syvenee. Arkeen ja työhön liittyvät toiminnot ja tiedot siirtyvät yhä laajemmin verkkoon.

Tietojärjestelmiin rekisteröidään yhä enemmän paikkaan, sijaintiin ja tapahtumiin liittyviä tietoja ja tietoja yhdistellään eri tarkoituksiin. Tietokannat laajentuvat ja tiedot eri järjestelmistä tulevat yhteiskäyttöisiksi. Samalla laajentuvat myös valvonnan ja väärinkäytön mahdollisuudet. Kansalainen on yhä haavoittuvampi.

Ubiikkiyhteiskunnassa tarvitaan yhä enemmän juuri kansalaisten edunvalvojaa. EFFI:n kaltaisten kansalaisjärjestöjen kannalta keskeisin trendi on se, että jatkossa poliittiset toimijat ovat yhä kiinnostuneempia tietojärjestelmien ja tietoverkon toiminnasta. Koska tietoteknologian toimintojen ala yhteiskunnassa jatkuvasti laajenee, yhä useammat asiat tulevat myös säätelyn alaiseksi.

Kansalaisten kiinnostus voi olla vaikeampaa herättää. Toistaiseksi lähinnä IT-lehdistön otsikoissa olevat tietojärjestelmien ongelmat tulevat olemaan iltapäivälehtien vakiomateriaalia ja saavuttavat laajemman yleisön. Tietotekniikkaan liittyvät yhteiskunnalliset ongelmat ja politiikka näkyvät kansalaisille medioiden kautta.

Medioiden kysymyksenasetteluihin reagoivassa politiikassa on vaarana se, jos poliittiset päättäjät vastaavat tilanteisiin luomalla lyhytjänteistä politiikkaa. Ratkaistaan välittömästi käsillä olevia konkreettisia tai yksittäisiä ongelmia, jotta median keskustelu rauhoittuu. Asian tarkastelu laajemmissa mittasuhteissa tai päätösten vaikutukset, jotka ulottuvat yhtä vaalikautta pidemmäksi ajaksi, voivat jäädä taka-alalle.

Ubiteknologian yleisenä ongelmana on asioiden monimutkaistuminen ja sen myötä vaikeus arvioida vaikutuksia ja mittasuhteita. Ubiikkiteknologian kytkökset, laajentumat ja yhteisvaikutukset eivät välttämättä ole nopeasti hahmotettavissa. Tämä on haaste kaikille päätöksenteossa mukana oleville tahoille, mutta myös kansalaisjärjestöille ja kansalaisille.

Tilanteesta koituu sekä mahdollisuuksia että ongelmia. Pluspuolella on, että teknologian arkipäiväistyessä siihen liittyvillä riskeillä ei voida enää myydä yhtä helposti poliittisia päätöksiä. Voidaan myös ennakoida, että teknologia tulee aiheuttamaan ennemmin tai myöhemmin erittäin näyttäviä tavallisten kansalaisten yksityisyyden loukkaamisia, mitä voidaan potentiaalisesti käyttää keinona nykyisen valvonnan lisääntymiskierteen katkaisemiseen.

Toisaalta jos järjestelmän ongelmat uhkaavat kansalaisten perusturvallisuutta (”jääkaappi ei toimi, kun siihen iski virus”), kuria ja järjestystä puoltavat voimat tulevat käyttämään tilannetta eittämättä hyväkseen. Valvontaa ja säätelyä on tähän saakkakin perusteettomasti myyty ja laajennettu perustellen sitä turvallisuuden lisääntymisellä.

Jos edellä mainitussa kilpailevien intressien taistelussa tulee tasapeli, jatkoajan tulee ratkaisemaan se, kuka koetaan ylimmäksi asiantuntijaksi teknisissä kysymyksissä. Ubiikkiyhteiskunnan teknisten syvärakenteiden sääntely näyttäisi olevan hyvin puhdasta asiantuntijavaltaa, jonka käyttö tapahtuu enemmän standardiorganisaatioiden kabineteissa kuin eduskunnan käytävillä. Näissä olosuhteissa EFFI:n kaltaisen järjestön lopullisen vaikutusvallan tulee ratkaisemaan sen aktiivien asiantuntemus.

Oikeudellinen tieto verkkoyhteiskunnassa

Ahti Saarenpää

Oikeudellinen tieto ja tietotekninen kehitys

Kun tietotekniikka tuli alun kokeilujen jälkeen yleisempään käyttöön 1950-luvulla, lausuttiin samalla syntysanat tulevalle tietopankkien aikakaudelle. Uusi tietotekniikka tarjosi mahdollisuudet laajamittaiselle informaation tallennukselle ja käsittelylle.

Oikeudellinen informaatio löysi varsin nopeasti tiensä erilaisiin tietopankkeihin. Oikeus on informaatiorikas yhteiskunnallinen aihepiiri ja oikeustiede on poikkeuksellisen informaatiorikas tiede. Tietopankit ovat siten luontevia oikeudellisen informaation tallennuspaikkoja. Sanavalintakin oli vielä tuolloin luonteva: pankkeihin luotettiin.

Matka yksittäisten tietokantojen ja tietopankkien käytön aloittamisesta ja niiden käyttöön vakiintumisesta on pitkä ja mutkikas. Siihen kuuluu koko joukko erilaisia historioita eri ammattikuntien tottumisesta tietotekniikan hyötykäyttöön. Niissä yhdistävinä tekijöinä ovat toisaalta ihmisten erilaiset yksilölliset valmiudet teknologian hyödyntämiseen ja toisaalta eri ammattitaitojen väliset jännitteet.

Oikeudellinen elämä eri muodoissaan on jo pitkään ollut sidoksissa tietotekniseen toimintaympäristöön, vaikka esimerkiksi oikeudellinen tiedonhaku ei vieläkään luontevasti kuulu kaikkien suomalaisten lakimiesten ammattitaitoon. Euroopan neuvosto havahdutti jo 1970-luvulla Suomenkin oikeusministeriön tietotekniikan tielle.

1990-luvun puolivälin tienoilla seuranta siitä, missä määrin lakimiehet käyttävät tietotekniikkaa ja tietopankkeja, lopetettiin esimerkiksi Yhdysvalloissa. Jokseenkin kaikki lakimiehet olivat tuolloin siirtyneet päätetyöläisiksi. Meillä kehitys on ollut huomattavasti hitaampaa. Sanelukone ja kynä kuluvat valitettavasti vieläkin monissa käsissä.

Oikeaa tietoa oikeaan aikaan

Tietokone ja tietopankki eivät pelkällä olemassaolollaan tuo lisäarvoa toimintaamme. Osaamattoman käsissä tai heikosti toimivina ne saattavat jopa vähentää toimintojen tehokkuutta. Lisäarvon tuottamiseen tar-

vitaan jotain enemmän: oikeaa informaatiota oikealla tavalla ja oikeaan aikaan.

Matka tuohon ideaaliin tavoitteeseen on pitkä ja vaikea. Kun kysymys on oikeudellisesta informaatiosta, se on tavallista vaikeampi. Oikeudellinen informaatio on tavanomaista tärkeämpää yhteiskunnallista informaatiota. Se liittyy tietoon oikeuksistamme ja valtaan, millä oikeuksiamme toteutetaan sekä rajoitetaan.

Oikeus on myös viestintää – vieläpä tavanomaista huomattavasti vaativampaa viestintää. Oikeudellinen viestintä kertoo, mikä on kulloinkin oikein, toivottua, sallittua, rajoitettua tai kiellettyä.

Oikeudellinen informaatio on lisäksi tärkeä oikeustieteellisen tutkimuksen kohde. Oikeusinformatiikka on muiden tehtäviensä ohella oikeudellista informaatiota ja tietojärjestelmiä tutkiva tiede. Sen lähtökohtana, etenkin Pohjoismaissa, on ollut ajatus oikeudesta merkittävänä yhteiskunnallisena viestintänä. Oikeusteoria ja oikeussemiotiikka tarkastelevat oikeutta myös viestintänä.

Lakien määrä lisääntyy ja lait monimutkaistuvat

Tarkasteltaessa oikeutta viestintänä, sen eräänlaisena ytimenä on lainsäädäntö. Elämme eurooppalaisessa oikeusvaltiossa – demokraattisessa oikeusvaltiossa. Sen keskeisiä tunnusmerkkejä on lakisääteisyys. Yhteisiä asioita järjestetään lakien avulla.

Perusoikeuksien merkityksen kasvaessa yksilön oikeuksista, niiden toteuttamisesta ja niiden rajoittamisesta on säädettävä lailla. Vain asetuksilla ja erilaisilla ohjeilla säätäminen ei riitä. Hallintovaltiolle aiemmin tunnusomainen viranomaisen yleistoimivalta on lähtökohtaisesti poistunut. Viranomaisen on oikeusvaltiossa voitava perustaa toimintansa lakiin.

Säänneltyjen asioiden ala myös laajenee. Lailla sääntelemättömät asiat ovat lainsäädännön lisääntyessä merkittävästi vähentyneet. Hallituksen eduskunnalle vuosittain antamista 200-300 lakiehdotuksesta osa koskee aina aikaisemmin lailla sääntelemättömiä asioita.

Lakien määrä ja merkitys yhteiskunnassa kasvavat jatkuvasti ja lainsäädäntö monimutkaistuu. Risto Heiskala on Anthony Giddensin ajatuksia jatkaen kuvannut tätä kehitystä puhumalla keinotekoisesta yhteiskunnasta. Jokseenkin kaikkea säädellään myös oikeudellisesti. Luonnollinen vaihtuu säännellyksi. Se, mikä on oikein, tunnistetaan usein vasta lainsäädännön välityksellä.

Lainsäädäntö on prosessin tulos

Lakiteksti on osa laajempaa oikeuden informaatioprosessia. Yhtä lailla tärkeitä asioita ovat lakien synty ja niiden soveltamiskäytäntö. Oikeuskäytännön myötä lain sisältö sekä sen merkitys saavat jatkuvasti uusia vivahteita.

Voimme puhua oikeudellisen informaation arvoketjusta. Sen lopputuloksena on käsitys siitä, mikä on oikein. Oikeusinformatiikka oikeudellisen informaation tieteenä seuraakin oikeudellisen tiedon tietä kattavasti alusta loppuun.

Lainvalmistelutyöt, lakiehdotusten eduskuntakäsittely ja oikeuskäytäntö ovat lakitekstin ohella tärkeitä elementtejä oikeudellisessa viestinnässä. Lisäksi oikeudellisella kirjallisuudella on tärkeä rooli oikeudellisten informaatiolähteiden kokonaisuudessa.

Voimme puhua eräänlaisesta oikeudellisen viestinnän kehästä. Se avataan usein yksittäisen lakitekstin avulla, mutta kysymys on laajemmasta informaatiokokonaisuudesta, joka kasvaa ja muuntuu koko ajan. Toki lakiteksti itsessään se lähtökohta, mihin tulee voida luottaa.

Sääntelyn lopputulos ei ainoastaan olekaan tärkeää, vaan enenevässä määrin myös se, miksi tuollaiseen tulokseen on päädytty. Tämä on tärkeä osa nykyaikaisen kansalaisyhteiskunnan ajatusta. “Miksi” on yhä useammin ja yhä useammalle tärkeä kysymys lakitekstiä luettaessa.

Kohden parempaa lainsäädäntöä

Kun oikeutta ja sen informaatioprosesseja tarkastellaan viestinnän näkökulmasta, on välttämätöntä aina muistaa myös viestinnän monet riskit. Osmo A. Wiion jo vuosikymmenten takainen, Wiion laeiksi luonnehdittu luettelo viestinnän ongelmista on edelleen ajankohtainen. Wiion laeista ensimmäinen soveltuu kärjistyksenä hyvin myös oikeudelliseen viestintään: viestintä yleensä epäonnistuu paitsi sattumalta.

Lain ja tuomioiden kirjoittamisen lähtökohta – ei mitään liikaa, ei mitään liian vähän – on viestinnän näkökulmasta ongelmallinen. Viestien vastaanottajien valmiudet viestien ymmärtämiseen vaihtelevat merkittävästi.

Viime vuosina on puhuttu paljon lainvalmistelun laadusta. Sitä on moitittu ja tavoitteena on nykyistä parempi lainsäädäntö. Parannusta asiaan on tuonut paremman sääntelyn toimintaohjelma, jolla tavoitellaan entistä johdonmukaisempaa säädöspolitiikkaa. Keväällä 2007 valmistui ehdotus säädösvalmistelun arvioinnin ohjeiksi. Oikeusministeriön sivuilla avattu paremman sääntelyn sivusto on myös kehityksen tulosta.

Suomi ei ole yksin pyrkimyksessään parempaan lainsäädäntöön. Tavoite on näkyvästi yleiseurooppalainen. Euroopan unioni massiivisena lainsäädännön tuottajana on yhtä lailla huolissaan sääntelyn laadusta. Ennen kaikkea lainsäädännön monimutkaistuminen nähdään EU:ssa ongelmana.

EU:n paremman sääntelyn toimintaohjelmassa pyritään esimerkiksi yksinkertaistetumpaan uudelleensäätämiseen sekä muuhun kuin sitovaan lainsäädäntöön. Toisaalta EU:n korostama oikeusvaltion ajatus asettaa tähän rajoja. Ohjeellinen sääntely avaisi helposti tien oikeuden ja talouden suhteen vääristymille.

Lakien sisältö pirstaloituu

Oikeaa viestiä on usein vaikeaa löytää säädösviidakosta. Yksittäinen laki siihen liittyvine tietoineen on aina osa laajempaa oikeusjärjestyksen kokonaisuutta. Kokonaisuus on monimutkaisessa ja monien toimijoiden lainsäädäntöprosessissa herkkä sirpaloitumaan.

Yhteiset käsitykset muuttuvat helposti erilaisiksi. Esimerkiksi tietosuojasta säätäminen on sirpaloitunut satojen erilaisin tavoittein säädettyjen säännösten epäyhtenäiseksi kokonaisuudeksi. Samaan asiaan on keväällä 2007 kiinnitetty huomiota Ruotsissa. Yksilön persoonallisuuden suojan (integritet) sääntelyä tutkinut komitea moittii lainvalmistelua heikosta laadusta – sen katsottiin kadottaneen yhtenäisen käsityksen ihmisen yksityisyydestä.

Oikeudellisen viestinnän keskeisiä kysymyksiä ovat, miten oikeudellisen tiedon tie lainvalmistelusta lain soveltamiseen kulkee, ja mitkä tekniset, tiedolliset ja taidolliset seikat voivat heikentää lain laatua. Kysymys ei ole vain lakiehdotusten yleisten vaikutusten arvioinnista, vaan koko informaatioprosessin laadusta.

Esimerkiksi Chilessä parlamentin kirjasto liittää lakiehdotuksiin lakimieskoulutuksen saaneiden kirjastonhoitajien toimesta tärkeää oikeuslähdeaineistoa, jotta parlamentti ei saisi puutteellista tai väärää kuvaa käsiteltävänä olevista asioista. Vaikka lainvalmistelu Chilessä on toisentyyppistä kuin meillä, toimintatavan käyttöönotto lainvalmistelun avoimuuden turvaamiseksi olisi kokeilemisen arvoista. Suomessa Eduskunnan kirjasto ja valtioneuvoston tietopalvelut ovat kehittäneet lainvalmisteluun hieman vastaavantyyppistä tietotukea. Sen lähtökohtina ovat kuitenkin olleet lainvalmistelijoiden puutteelliset tiedonhakuvalmiudet. (http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/03_tyoryhmamuistiot/20060922Saeaedoes/palmen_NETTI_21_09_2006.pdf)

Oikeudelliset tietovarannot

Timo Kuronen on tuonut käyttöömme tietovarannon käsitteen. Kuroselle tietovaranto on ensi sijassa tietoverkkojen avulla käytettävä, yhteiskunnallisesti merkittävä informaatiokokonaisuus. Käsite on sittemmin levinnyt vähemmän tärkeidenkin kokonaisuuksien kuvaajaksi.

Oikeudellinen tietovaranto epäilemättä kuuluu yhteiskunnallisesti tärkeisiin tietovarantoihin. On oikeutettua puhua yhdestä välttämättömästä perustietovarannosta, joka on oltava ja johon on voitava luottaa. Se kuuluu oikeusvaltioon.

Perustietovarannot ovat jo useissa maissa suurelta osin verkossa. Tähän on edetty monen vaiheen kautta. Suomessa oikeudellisen perustietovarannon verkkoaika sai alkunsa 1980-luvun alussa. Vuonna 1982 oikeudellinen tietopankki Finlex avattiin yleisempään online-käyttöön.

Taustalla oli Euroopan neuvoston suositus oikeudellisten tietopankkien kehittämisestä. Suomi ei ollut Euroopan neuvoston jäsenmaa, mutta oikeusministeriössä seurattiin sen toimintaa tärkeänä eurooppalaisena oikeudellisen kehityksen arvioijana ja tiedon tuottajana.

Finlexin alkuperäinen perusajatus oli varsin onnistunut. Sen puitteisiin koottiin yhteen keskeistä oikeuslähdemateriaalia hyödynnettäväksi yhden tiedon tallennus- ja hakuohjelmiston, Mintun, avulla. Näiltä juurilta se ehti kasvaa noin 40 tietokannan merkittäväksi perustietovarannoksi. Olimme, kiitos ennen kaikkea hovioikeuden presidentti Martti Leisténin varhaisen valistuneisuuden, eurooppalaisittainkin kehityksen kärjessä.

Alkuperäisen Finlexin rasitteina olivat sen käytön maksullisuus ja yhtenäisen dokumenttituotannon puute. Tuomioistuimille sekä oikeushallinnolle maksuttomana ja muille maksullisena, Finlex vinoutti oikeudenmukaiseen oikeudenkäyntiin kuuluvaa asianosaisten informaatiotasapainoa. Dokumenttien erilaisuus puolestaan vaati usein informaation ja sen päätekäyttäjän välille avustavaa henkilöstöä. Tämä hintavaksi käynyt hankaluus oli yksi tietopankin käytön yleistymisen esteistä. Alkuperäinen Finlex oli lähinnä taitavan käyttäjän tietopankki.

Nykyisin vapaaseen verkkokäyttöön on tarjolla maksuton Finlex. Se on kuitenkin aikaisempaa huomattavasti suppeampi. Matkalla verkkoyhteiskuntaan on saavutettu ja menetetty jotain merkittävää.

Maksuttomat oikeudelliset perustietovarannot

Siirtymä maksuttomuuteen ei ollut helppo. Julkinen valta pyrki rahastamaan perustietovarannoilla ja käytössään olevilla tiedoilla.

Matka julkisen sektorin tietojen avointa käyttöä koskevaan eurooppalaiseen direktiiviin oli pitkä ja kivinen. Sitä pyrittiin tekemään enemmän markkinoiden kuin ihmisen oikeuksien näkökulmasta. Direktiivi, jonka tavoitteena oli edistää julkisen sektorin tietojen avointa käyttöä ennen kaikkea sähköisessä muodossa, saatiin lopulta hyväksytyksi vuonna 2003.

Suomessa suuntaa muutettiin jo merkittävästi aiemmin. Kun valtiopäiväasiakirjat ja Eduskunnan kirjaston tietokannat tuotiin maksutta avoimeen tietoverkkoon vuoden 1995 lopulla, tehtiin suomalaista oikeudellisen tietohuollon ja tietovarantojen historiaa. Siinä Eduskunnan kirjaston hallituksen kokouksessa, missä tuo avaus virallisesti todettiin, oli mukava istua. Eduskunta käveli ihmisen hyväksi kepeästi valtionvarainministeriön ylitse kohden verkkoyhteiskuntaa ja demokraattista oikeusvaltiota.

Finlexin maksuttomuuden aika alkoi vuonna 1997. Se ei yksinkertaisesti voinut enää jäädä maksulliseksi. Perustietovarannon keskeiset osat eivät saisi ollakaan keskenään erilaisessa asemassa.

Oikeudellisen tiedonhaun ongelmat

Oikeudellinen perustietovaranto on kehityksen myötä myös pirstoutunut. Se on muuttunut osin tietopankin ulkopuolisiksi ja eri tavoin ylläpidetyiksi selattaviksi kotisivuiksi. Esimerkiksi tekijänoikeusneuvoston ja tietosuojavaltuutetun ratkaisut ovat näiden instituutioiden kotisivuilla.

Tietovarantojen eriytyminen on kiistämätön menetys. Oikeudellinen perustietovaranto ei ole edes virallistiedon osalta kokonaisuus. Tiedon tuottaminen kotisivuille on joustava, halpa ja tietoteknisten välineiden helposti tukema ratkaisu. Käyttäjiä hankaloittaa kuitenkin tiedon tavoittaminen eri lähteistä.

Yleisempi tietovarantojen kehitykseen liittyvä ongelma on hakukielen näkymättömyys. Alkuperäisen Finlexin käyttäjän piti tuntea hakukieli ominaisuuksineen. Nykyinen Finlex on tyypillinen hakulomakkeille rakentuva tietokanta.

Oikeudellisen informaatiolukutaidon heikkous korostuu yksinkertaisessa lomakehaussa. Finlex houkuttelee selainten tavoin etsimään informaatiota pinnallisesti yksittäisin hakusanoin, mikä hakutapana tuottaa puutteellisia hakutuloksia.

Tiedonhakijan olisi tunnettava sisällöissä käytetty oikeuden kieli. Vastaavasti oikeuden toimijoiden olisi käytettävä yhtenäistä kieltä, jotta kaikki aiheeseen liittyvät sisällöt löytyisivät. Kumpikin tavoite on käytännössä jäänyt hyvin etäiseksi.

Oikeudellinen tieto on sosiaalista pääomaa

Timo Kurosen tavoin on syytä muistuttaa perustietovarantojen yhteiskunnallisesta merkityksestä. Niitä luonnehditaan taloudellisesta näkökulmasta myös tuotannontekijöiksi.

Perustietovarannot ovat kuitenkin enemmän. Ne liittyvät olennaisella tavalla demokraattisen oikeusvaltion kehitykseen ja ylläpitoon. Voimme puhua, kuten esimerkiksi Wirginia Wise ja Frederick Schauer ovat tehneet, sosiaalisesta pääomasta.

Oikeudellisen perustietovarannon keskeiset periaatteet ankkuroituvat jo mainittuihin kahteen keskeiseen peruspilariin: demokratiaan ja viestintään. Kansalaisten näkökulma on erityisen tärkeä. Kansalaisen on voitava ymmärtää omia oikeuksiaan ja velvollisuuksiaan. Oikeudellinen perustietovaranto on siinä suhteessa erityinen, että sen ensisijainen käyttäjä on yksittäinen kansalainen, eivät ammattikunnat tai markkinat.

Tuomas Pöysti onkin osuvasti todennut kommenttina valtiontalouden tarkastusviraston tekeillä olevaan lainsäädäntösuunnitelmaan, että

> ”oikeus lain ja oikeuden ymmärtämiseen on kansalaisen perusoikeus ja perusta aktiiviselle kansalaisuudelle”.

Ajatusta on syytä täydentää vanhalla, mutta edelleen velvoittavalla lain tuntemuksen vaatimuksella. Kansalaisen on tunnettava laki. Sen tuntemattomuus ei ole anteeksiantoperuste: ”ignorantia iuris nocet”.

Verkkoyhteiskunnassa periaate voi muuttua paljon käytännönläheisemmäksi, jos oikeudellisten perustietovarantojen kehittämisen ja ylläpidon periaatteet saadaan kehitettyä kansalaisen oikeuksia vastaaviksi.

Miten oikeudellinen tieto löytää lukijan?

Oikeudellisten tietovarantojen periaatteista on kansainvälisesti keskusteltu esimerkiksi OECD:n toimesta. OECD:n ohje lainsäädännön laadusta vuodelta 1995 on tärkeä kansainvälinen dokumentti. Lähemmin asiaa on sittemmin tarkasteltu oikeusinformatiikan puitteissa.

Kansalaisten ja virallisinformaation kannalta ainakin seuraavat seitsemän periaatetta osoittautuvat merkityksellisiksi: informaation saatavuus, oikeellisuus, tavoitettavuus, haettavuus, ymmärrettävyys, käytettävyys ja halpuus.

Saatavuus

Virallisinformaation saatavuudella tarkoitetaan sen julkisuutta. Pohjoismaisessa julkisuusajattelussa virallisaineisto on julkista, ellei toisin määritellä erityisien salassapitosäännöksien tai yksityisyyden suojan takia. Oikeudellisen perusinformaation tulisi myös olla mahdollisimman täydellisenä saatavissa. Näin ollen sellaisten dokumenttien, missä on esimerkiksi henkilötietolain tai julkisuuslain mukaan salassa pidettävää tietoa, tulisi olla vain näiltä osin salaisia.

Pohjoismaisesta näkökulmasta informaation saatavuus itsessään on selkeä tietovarantoperiaate. Se on selkeämpi kuin monissa muissa Euroopan maissa.

Saatavuuden toteuttamiseen liittyy kuitenkin ongelmia. Asioiden salassapito ja toisaalta niistä tiedottaminen voivat aiheuttaa informaatioepätasapainoa. Kokonaisten dokumenttien salassapito johtaa siihen, että myös asiat, joiden ei pitäisi olla salaisia, jäävät vaille asianmukaista julkisuutta. Syntyy eräänlaista salaista lainsäädäntöä, mikä on demokratialle vieras periaate.

Kasvavan ongelman muodostaa se, että toistaiseksi puuttuu dynaamisen, eri tarkoituksiin muuntuvan julkisen asiakirjan käsite. Vaikka tekstinkäsittelystä on julkisella sektorilla pääosin siirrytty asiankäsittelyyn ja dokumenttituotantoon, dokumentit sinänsä eri toimien lopputuloksina edustavat edelleen staattisen dokumentin ajatusta.

Asiakirjaksi luetaan julkisuuslain mukaan alustalle merkitty viesti. Siten esimerkiksi lokitiedot ovat asiakirjoja, mutta päätökset tuotetaan edelleen kokonaisdokumentteina. Salassa pidettävät henkilötiedot ja liikesalaisuudet tuottavat myös käytännössä jatkuvia muun tiedon saatavuusongelmia, jos salaisia tietoja sisältyy osina laajempiin tai merkityksellisiin asiakirjoihin.

Viranomaisten tiedottaminen oikeudenkäynnin tai hallinnollisen asian eri vaiheissa saattaa johtaa asianosaisille, erityisesti rikosasioiden syytetyille, haitalliseen informaatioepätasapainoon. Pahimmillaan tästä seuraa kaksi oikeudenkäyntiä: virallinen ja epävirallinen (trial by media). Oikeudelliset ja sosiaaliset normit kulkevat eri tahdissa.

Erään saatavuusongelman aiheuttaa oikeutemme anonymiteettiin. Kansalaisella on oikeus saada virallista tietoa anonyymisti. Tuon keskeisen oikeuden tulisi toteutua myös verkkotiedonhaussa, vaikka sitä ei aina havaita. Kun esimerkiksi pyritään tietoturvattuun viestintään yksilön vahvan tunnistamisen avulla, tulisi tiedonhausta viranomaisen tietojärjestelmään jäävien jälkien käsittelyssä toisaalta taata tiedonhakijan anonymiteetti.

Viime vuosien oudoin anonymiteetin loukkaus tapahtui otettaessa aikanaan käyttöön Finlexin ajantasainen säädöstietokanta. Sen käyttö edellytti aluksi käyttäjän rekisteröitymistä. Saadakseen tietää digitaalisesti, mikä on lain sisältö, ihmisen tuli kertoa, kuka hän on. Ja asialla oli oikeusministeriö. Huh!

Oikeellisuus

Informaation oikeellisuuteen joudutaan kiinnittämään erityistä huomiota. Tiedon tie sen tallennuksesta käyttöön ja edelleen arkistoitavaksi tai hävitettäväksi on pitkä ja avointen tietoverkkojen vuoksi myös turvaton.

Kansalaisilla on luonnollisesti oltava oikeus luottaa siihen, että virallisinformaatio on virheetöntä sisältönsä ja kattavuutensa puolesta. Oikeellisuus on kriittistä esimerkiksi silloin, kun dokumentin sisällönkuvaus johtaa vääriin tuloksiin tiedonhaussa. Oikeellisuutta voidaankin pitää yhtenä sosiaalisen pääoman ominaisuuksista.

Toistaiseksi valtiovalta Suomessa on lähtenyt siitä, että se vastaa vain perinteisessä painetussa muodossa oleva informaation, erityisesti säädösten, oikeellisuudesta. Sen sijaan sähköisen informaation yhteyteen sijoitetaan yleensä erilaisia vastuuvapauslausekkeita. Niiden merkitys on vähitellen käymässä kyseenalaiseksi viranomaisten toimintaan kohdistuvien laatuvaatimusten kasvaessa. On myös erikoista, että sähköisen virallisinformaation käytön kasvaessa sille ei ole toistaiseksi asetettu välittömiä laillisia virheettömyysvaatimuksia.

Tavoitettavuus

Virallisinformaation tavoitettavuudella tarkoitan sitä, että virallisaineisto on hyödynnettävissä mahdollisimman ajantasaisena ja alueellisista, erilaisista tallennustavoista tai kustannuksista muodostuvista kynnyksistä vapaana.

Heikko tavoitettavuus vähentää informaation saatavuuden merkitystä. Jopa painetun säädöskokoelman toimittaminen asiakkaille kakkosluokan postissa on varhemmin aiheuttanut ongelmatilanteita. Tämän päivän ongelma on julkisen sektorin toistaiseksi vaatimaton ennakkotiedottaminen säädösmuutoksista.

Verkkopalvelut epäilemättä alentavat alueellisen tavoitettavuuden kynnystä ja vähentävät eriarvoisuutta. Siitä hyötyvät ensi sijassa tietoverkkojen aktiivikäyttäjät, joiden määrä on kasvussa.

Painetussa muodossa olevan virallisinformaation tavoitettavuus tulee kuitenkin vielä pitkään olemaan yksi oikeusvaltiokehityksen ongelmis-

ta. Kaikki materiaali ei vieläkään ole verkossa. Lisäksi viranomaisten tietojärjestelmien erilaisuus on merkittävä verkkoviestinnän ongelma.

Haettavuus

Haettavuus on kaiken tiedonvälityksen lähtökohtia. Siihen on perinteisesti pyritty esimerkiksi kirjastoissa kirjallisuuden indeksoinnin ja asiasanoituksen avulla. Vastaavasti eri maiden säädöskokoelmat ovat tärkeitä välineitä oikeudellisessa viestinnässä. Saatavuus ja tavoitettavuus eivät riitä, mikäli itse tietovarasto on vailla riittävää järjestystä.

Suomessa keskeisen lakikirjamme, Suomen Lain, systematiikka ja erilaiset viittaukset ovat olennainen osa oikeuskulttuuria. Yhdysvalloissa johtavassa markkina-asemassa pitkään olleen West Lawn luokitusjärjestelmän on arvioitu olleen jopa oikeusjärjestelmää ohjaava tekijä. Robert C. Berringin käynnistämä keskustelu asiasta on merkille pantava myös meillä Suomessa.

Verkkoympäristössä informaation haettavuudella on entistä tärkeämpi rooli. Voimme puhua siitä ainakin neljässä eri merkityksessä: (1) tietopankkien ja tietokantojen, (2) dokumenttien, (3) dokumenttien eri osien sekä viime kädessä (4) tekstin, merkkien ja kuvien haettavuutena.

Avoimia tietoverkkoja hyödynnettäessä ensimmäinen haettavuusongelma ilmenee, jos emme tunne tietopankkien tai tietokantojen tarkkoja nimiä tai osoitteita. Yleisiä hakukoneita käytettäessä tärkeät oikeudelliset tietokannat saattavat jäädä huomaamatta.

Hidasta havahtumista verkkoyhteiskunnan haettavuusongelmiin kuvaa hyvin se, että Suomessa ministeriöillä ja muilla viranomaisilla ei ole ollut yhtenäistä verkko-osoitteiden nimeämistapaa. Jopa eri ministeriöiden verkko-osoitteet on valittu epäyhtenäisellä tavalla. Siksi haettavuuden ongelmia pyritään hälventämään ala- ja aihekohtaisin portaalein ja linkkilistoin. Maakohtaiset viralliset portaalit, kuten Suomi.fi, ovat merkinneet julkisen sektorin osalta askelta eteenpäin.

Erilaisten linkkilistojen ongelmana on epävarmuus laadusta. Kaikilla linkkilistojen ylläpitäjillä ei ole riittävää ammattitaitoa tietokantojen tärkeyden arviointiin, eikä toisaalta resursseja linkkilistan päivityksiin. Linkkilista on hyvä apuväline, mutta yhteen linkkilistaan luottaminen on huono ratkaisumalli.

Esimerkiksi kansainvälistä oikeudellista tietoa etsittäessä Eduskunnan kirjaston ELKI:n lisäksi olisi käytettävä ruotsalaista Rättvisarea ja norjalaista Jurisdisk nettviseriä. Silloinkin ollaan vasta tiedon tien alkupäässä. Tietosuojaan liittyvän informaation yhtenä luontevana hakuväylästönä taas

toimivat eri maiden tietosuojaviranomaisten sivut linkkilistoineen.

Dokumenttien eri osien haettavuus on viime kädessä kiinni siitä, hyödynnetäänkö mahdollisuuksia rakenteisiin dokumentteihin. Tiedonhakijalta edellytetään silloin riittävää dokumentin rakenteiden tuntemusta. Yksittäinen hakusana hakulomakkeella dokumenttirakennetta tuntematta on yleensä ja erityisesti oikeudellisessa tiedonhaussa huono hakutapa. Harva tiedonhakija kuitenkaan tuntee rakenteisuuden merkitystä, eikä siitä välttämättä kerrota sivuilla. Tietoa on osattava hakea oikeista kentistä tai oikealla hakutavalla.

Haettavuuden on perinteisesti ajateltu riippuvan tekstistä itsestään. Oikeudellisten tekstien luonteesta ja oikeuslähdeopista johtuen vapaa tekstihaku kokotekstidokumenteista on nähty ensisijaiseksi hakutavaksi oikeudellista informaatiota etsittäessä. Hakusanat ja luokitukset saattavat sulkea merkittävää informaatiota pois hakutuloksista. Esimerkiksi yksittäinen oikeustapaus saattaa sisältää yhden tai useamman laveamman oikeusperiaatteen, mikä jää havaitsematta suppeaan luokitukseen tai muutamaan hakusanaan turvauduttaessa. Niukat hakusanat voivat helposti johtaa tiedonhakijan vääriin käsityksiin asioista.

Tekstihaku kokotekstistä asettaa myös kielet vastakkain: tiedon tuottajan kielen ja tiedonhakijan kielen sekä yleiskielen. Jos ne eivät kohtaa, tiedonhaku ja sen tulosten hyödyntäminen saattavat epäonnistua. Yksityisyys (privacy) ja tietosuoja (data protection) ovat havainnollisia esimerkkejä käsitteistä, joiden yleisyys tekee ne etenkin englanninkielisessä tiedonhaussa erottelukyvyttömiksi.

Poikkeuksiakin toki on hakukoneisiin liittyen. Esimerkiksi yhdistelmä “EU data protection” vie meidät Googlen myötä eurooppalaisen tietosuojan perussivuille eli komission “Freedom, security and justice” -sivuille. On hyvä, että henkilötietojen suoja on komission sivuilla nyt systemaattisesti oikeammassa paikassa. Aikaisemmin sen kotipesänä oli EU:n perinteisen luokittelun mukaisesti, mutta harhaanjohtavasti, sisämarkkinoiden internal market -sivusto.

Verkkoympäristössä tärkeäksi on noussut myös dokumenttien kuvauskieli eli se kieli, jolla tietoa tallennetaan tietokantoihin tai verkkosivuille. Tiedon tie alkaa todellakin siitä, millaista merkintätapaa ja merkintäkieltä tiedon tuottaja käyttää. Yhtenäisillä merkintätavoilla vaikutetaan merkittävästi tiedon haettavuuteen. Tähän oikeudellisen tiedonhaun tutkimuksessa ja opetuksessa ei ole kiinnitetty riittävästi huomiota. Eräät kansainväliset tutkimus- ja yhteistyöprojektit, kuten Legal XML ja siihen liittyen Lisa pyrkivät kuitenkin standardien luomiseen.

Ymmärrettävyys

Ymmärrettävyys on viimein kaiken oikeudellisen informaation perusvaatimus. Kysymys ei kuitenkaan ole vain kielestä, vaan yleisemmistä viestinnän peruselementeistä, jotka ovat sekä kansallisia että kansainvälisiä.

Virallisen oikeuslähdeaineiston tulee olla tekstin ja ulkoasun sekä viitteidensä ja selostuksien puolesta mahdollisimman laajalti ymmärrettävissä. Tässä on verkkoyhteiskunnan aito ja syvenevä ongelma.

Oikeuden kohtauspaikka on muuttumassa. Siinä missä ensisijaisesti lakimies tai virkamies ennen luki lakitekstiä, sen lukee nyt yhä useammin kansalainen. Ilmiö on kansainvälinen. Tähän ei oikeudellisten tekstien tuottamisessa ole varauduttu.

Lait tehdään edelleen käsityönä ilman vakiintunutta sanastoa. Vaikka esimerkiksi korkein oikeus on EY-tuomioistuimen mallin mukaisesti selventänyt tuomioiden kirjoitustapaa, kielellinen kokonaiskuva eri tuomioistuinten tuomioista ja hallintoviranomaisten ratkaisuista on valitettavan epäjohdonmukainen. Se on ilmeistä seurausta tietojohtamisen puutteesta. Siksi esimerkiksi tuomioiden monisanainen perustelemattomuus on yksi aikamme näkyvistä oikeudellisista ilmiöistä.

Oman periaatteellisen ongelmansa aiheuttaa se, että tuomioistuinten ennakkoratkaisut ovat yksikielisiä. Niitä ei käännetä muille virallisille kielillemme lyhyitä otsikoita tai selosteita lukuun ottamatta. Se on ongelma kielellisille vähemmistöryhmille.

Oikeusvaltiossa on entistä tärkeämpää myös se, miltä oikeudellinen informaatio näyttää. Se on osa oikeuden välttämätöntä arvokkuutta. Joudutaan esimerkiksi kysymään, millaisia oikeuden kuvia ja merkkejä oikeuslähdeaineistoon tulee tai voidaan liittää. Näitä kysymyksiä on toistaiseksi kansainvälisestikin tutkittu harvinaisen vähän. Siinä missä liikennemerkit on havaittu välttämättömiksi oikeuden merkeiksi, muita kuvia ja merkkejä ei juuri ole. Medialle oikeuden kuva on useimmiten lakikirjan selkämys tai kansi.

Oikeudelliset tekstit ovat edelleen paperialustalle tarkoitettuja lineaarisia tekstejä. Tuomioistuinten tuomioissa ja laillisuusvalvojien ratkaisuissa ei meillä käytetä oikeustieteessä tavanomaisia, lukemista helpottavia alaviitteitä. Silloin kun viitteitä ylipäätään käytetään, ne ovat, esimerkiksi Eduskunnan oikeusasiamiehen ratkaisuissa, sisäisiä viitteitä. Sellaiset yleensä heikentävät tekstin luettavuutta katkaistessaan normaalin lineaarisen tekstin.

Käytettävyys

Käytettävyys on tietovarannoille tärkeä vaatimus. Kysymys on siitä, miten informaatio voidaan siirtää tietovarannosta käyttäjän omiin järjestelmiin. Tiedon tie jatkuu käyttäjän omissa järjestelmissä. Puhumme myös informaatiologistiikasta.

Käytettävyyteen vaikuttavat merkittävästi ne standardit, joita käyttäen informaatio on merkitty dokumenttijärjestelmiin. Toistaiseksi käytettävyys on ollut vaatimatonta, mistä aiheutuu paitsi hankaluuksia myös riskejä informaation muuntumiselle, kun sitä siirretään tietojärjestelmästä toiseen.

Tyyppiesimerkkinä käytettävyysongelmasta on se, että informaatiota kopioitaessa, sitä usein seuraa merkittävä määrä erilaisia näkymättömiä koodimerkintöjä. Finlexin käytettävyyttä on parannettu vuoden 2006 lopulla lisäämällä siihen mahdollisuus tiedonhakuun suoraan Word-, PowerPoint- ja Excel -ohjelmistojen sisältä. Tämän myönteisen muutoksen varjopuolena on, että tiedon hyödyntäminen yhdistyy yksittäisen ohjelmistoyhtiön tuotteisiin. Käytäntö on vaikeasti sovitettavissa julkisen vallan tehtäviin.

Halpuus

Seitsemäs oikeudellisten tietovarantojen arvioinnin ja kehittämisen vaatimus on informaation halpuus. Se koskee yleisemmin kaikkea merkittävää oikeudellista tietoa. Kysymys on sosiaalisen pääoman käytöstä. Oikeudellisen perustietovarannon virallisaineiston käytön tulisi olla ilmaista.

Halpuuden vaatimus perustuu kahteen keskeiseen demokratian perusperiaatteeseen: oikeus tietoon sekä tiedon vapaus. Meillä on demokratiassa oikeus tietoon. Se on samalla yksi informaatio-oikeuden keskeisistä periaatteista.

Oikeutta tietoon toteutetaan tiedon vapaan kulun (free flow of information) avulla. Tämän mukaisesti on perusteltua odottaa, että virallinen informaatio on ensisijaisesti ilmaista. Vastaavasti julkisen informaation ilmaisuus tukee sen varaan rakentuvan kaupallisen oikeudellisen informaation halpuutta.

Julkinen valta ei saisi rahastaa kansalaisia sillä, minkä se velvollisuuksiensa puitteissa joutuu tekemään tietovarantoja ylläpitäessään. Kysymys on, kuten Timo Kuronen on sattuvasti todennut, julkishyödykkeistä. Niiden perusominaisuuksia on väistämättä halpuus.

Samaan yhteyteen kuuluu kysymys tietoverkkojen käytön hinnasta.

Kun kysymys on yleisestä informaatioinfrastruktuurista, sen käytön tulisi olla edullista. Tähän on havahduttu eurooppalaisella tasolla kovin myöhään. Esimerkiksi “e-Europe 2005” -politiikkaohjelman tavoitteena kuitenkin on nyt avointen verkkojen edullinen käyttö. Se on välttämätön osa yleisen informaatioinfrastruktuurin kehittämistä verkkoyhteiskunnassa.

Oikeus ja sen tulkinta verkoissa

Oikeudellisesta tietovarannosta puhuessamme on muistettava, että oikeus on itse asiassa joukko kertomuksia siitä, mikä on tai minkä tulisi olla oikein. Tekstejä tulkitaan, niitä yhdistetään ja niitä verrataan. Tämä on keskeinen osa lakimiestaitoa.

Usein on kuviteltu lakitekstien olevan ennen kaikkea lakimiehiä varten. Vasta he kertovat muille, mikä on oikein. Juuri heille oikeustiede esittää tulkintasuosituksiaan. Lakimiesten ammattikunta hallinnoi oikeudellista tietoa.

Ajatus on vaarallinen, sillä se sivuuttaa yksioikoisesti kansalaiset. Kysymys on demokraattisessa yhteiskunnassa aina ensisijaisesti yksilön oikeuksista ja heidän oikeuksistaan tietoon. On esitetty ajatus, että normien määrän lisääntyminen ei ole kovinkaan huolestuttavaa, koska suuri osa niistä koskee hallintoa, mutta ei kansalaisia. Päätelmä on virheellinen. Kansalaisilla on oikeus tietää, mitä hallinnosta on säädetty ja miten se toimii. Myös hallintoa koskevalta lainsäädännöltä edellytetään samaa ymmärrettävyyttä kuin muulta lainsäädännöltä. Muutoin yhteiskunta ei olisi avoin.

Kansalainen lakitekstien lukijana

Oikeudellinen tieto avoimissa verkoissa tuo eteemme uuden tilanteen lakia luettaessa. Yhä useammin lakitekstin ensisijainen hyödyntäjä on kansalainen. Lakimies tai muu asiantuntija viestin ensisijaisena vastaanottajana jää sivuun tai sivummalle.

Tekstejä luetaan ilman oikeudellista ammattitaitoa. Tämäkin on luonnollinen osa demokratiaa. Yksilön oikeuden tulee olla ihmisen ymmärrettävissä.

Demokraattisessa oikeusvaltiossa lainsäädännön tulisi olla osa sosiaalista pääomaamme. Tätä ei ole juurikaan muistettu esimerkiksi pohdittaessa tuomioistuinlaitoksen kehittämisen yhteydessä tuomarin työn vaativuutta.

Oikeuden kohtauspaikan muuttuminen asettaa kasvavia laatuvaatimuksia oikeudelliselle perustietovarannolle. Tätä ei ole parempaan lainsäädäntöön pyrittäessä toistaiseksi havaittu.

Muutos asettaa myös lakimieskunnan uusien laatuvaatimusten eteen. Emme enää tarvitse niitä lakimiehiä, joiden palvelutehtävä on perustunut vain sen oikeuslähdeaineiston hallussapitoon, joka nyt on maallikon silmien edessä verkossa. Tarvitaan pidemmälle menevää taitoa ja välineitä kertoa, mikä ja miksi kulloinkin on oikein.

Perustietovarannon muuttuneet käyttötilanteet merkitsevät myös uutta haastetta markkinoille. Tarvitsemme lisää sellaisia tietotuotteita, missä virallisen perustietovarannon sisältöä selostetaan syvemmin. Oikeustieteellisen kirjallisuuden lisäksi tarvitaan selostavaa ja helppolukuista oikeudellista kirjallisuutta. Sitä on, mutta vailla yhtenäisempiä laatutakeita.

Lakitekstien käsitteet ja oikeuslähdeoppi

Lakimiehet luovat kertomuksia oikeasta ammattikuntansa yhdistävien teorioiden, periaatteiden ja käsitteiden avulla. Käsitteet ovat oikeudellisen lukutaidon kannalta keskeisessä asemassa. Kansalaiselle ne voivat osoittautua ylipääsemättömäksi esteeksi oikeudellisten tekstien ymmärtämiselle. Esimerkiksi sana tietosuoja voi johtaa maallikon harhaan. Tietosuojalainsäädäntö suojaa ensisijaisesti ihmistä, ei tietoja.

Käsitteet voivat olla laissa määriteltyjä, mutta merkittävä osa ensi sijassa oikeustieteen tuottamia. Uudemmalle lainsäädännölle on tyypillistä käsitemäärittelyiden esittäminen lain ensimmäisessä luvussa. Esimerkiksi henkilötietolaissa on 9 määritelmää ja sähköisen viestinnän tietosuojalaissa 17 määritelmää.

Lakien nimet ovat usein tiedonhaun esteenä. Lakien otsikoita luodaan edelleen monisanaisina, mikä samalla vaikeuttaa tiedonhakua. Julkisuuslaki esimerkiksi on viralliselta nimeltään “laki viranomaisen toiminnan julkisuudesta” ja holhoustoimilaki puolestaan “laki holhoustoimesta”. Kansalaiselle näiden lakien etsiminen on työlästä.

Finlex avustaa käyttäjää listaamalla joukon keskeisiä lakien nimiä sellaisina, kuin ne käytännössä esiintyvät. Harva kuitenkaan oivaltaa etsiä niitä otsikon “vakiintuneet säädösnimikkeet” alta. Ilmaisu “säädösnimike”, taitaa pikemminkin lisätä tiedonhaun tuskaa, kuin auttaa sen vähentämisessä.

Kertomuksia oikeudesta ohjaa keskeisellä tavalla myös oikeuslähdeoppi. Se kertoo, mitä oikeuslähteitä tulee ja on lupa käyttää oikeudellisia tulkintoja tehtäessä. Oikeuslähdeoppi kertoo myös, miten noita

lähteitä käytetään. Tämä on lakimiehen ydinosaamista.

Kaikki oikeuslähdeaineisto ei ole samanarvoista. Esimerkiksi säädännäiseen oikeuteen rakentuvassa oikeusvaltiossa meillä ei virallisesti tunneta sitovia ennakkoratkaisuja.

Hyvin tyypillinen kansalaisen tai toimittajan erhe on luulla ennakkoratkaisuja sitoviksi. Esimerkiksi verotuksen alueella niillä on pitkään ollut perustuslain tarkoittamaa keskeisempi käytäntöä ohjaava merkitys. Kun ennakkoratkaisut löytyvät nykyisin verkosta, niiden käytännöllinen merkitys on epäilemättä kasvamaan päin. Oikeuskirjallisuudessa näkyy myös ennakkoratkaisujen aikaisempaa laveampi määrällinen huomioiminen. Julkaisemistapa ja merkitys ovat suhteessa toisiinsa.

Kun ennakkoratkaisut eivät meillä sido, mutta niitä usein noudatetaan, on luonnollisesti tärkeää tietää, miten ennakkoratkaisuihin ja muuhunkin oikeuskäytäntöön oikeuskirjallisuudessa suhtaudutaan. Tähän tarjoaa merkittävän avun Finlexin FOKI eli oikeuskäytäntö kirjallisuudessa -tietokanta. Sen perusajatus on yksinkertainen – joku lukee puolestasi.

Oikeuskirjallisuudessa riittääkin luettavaa. Kesäkuussa 2007 FOKI -tietokannassa oli runsaat 607.000 viittausta noin 122.000 oikeustapaukseen. Finlexissä FOKI on löydettävissä oikeuskäytäntö-sivun alalaidassa. Se jää satunnaiselta sivuvierailijalta helposti huomaamatta sivun pituudesta johtuen. Tämäkin on yksi verkkoyhteiskunnan ongelmista - puutteellinen verkkoaineiston sivusuunnittelu.

Kansainvälistymisen vaikutukset

Oikeuslähdeopillisesti merkittävä virallinen muutos puolestaan liittyy oikeuden lähdesyvyyteen. Olemme eurooppalaisessa oikeusvaltiossa yhä enemmän sidoksissa ihmisoikeuksiin ja eurooppaoikeuteen. Kansallisessa lainsäädännössämme olemme myös huomattavassa määrin siirtyneet kansainvälisen taustan sekä sidonnaisuudet omaavaan lainsäädäntöön.

Perustieto ihmisoikeuksista ja eurooppaoikeudesta on nykyisin ennen kaikkea verkkotietoa. Se on helposti löydettävissä, mutta edellyttää, että tiedonhakija tuntee EU:n päätöksenteon rakennetta sekä erilaisten tietovarantojen ominaisuuksia.

Kriittiset puheet siitä, että EU ei olisi avoin, voidaan oikeudellisen tiedon osalta unohtaa. EU on yksi maailman merkittävimmistä oikeudellisen tiedon tuottajista. Se aika on ohi, jolloin virallisia asiakirjoja koottiin harvoihin EU-tallekirjastoihin ja niitä pidettiin tuon tiedon merkittävimpinä tietovarastoina. Keskustelua asiakirjojen saatavuudesta ja

sisällöstä jatketaan edelleen esimerkiksi EU:n avoimuusasetukseen liittyvän ns. vihreän kirjan pohjalta.

Eurooppatiedon laadun parantamisessa Euroopan unionilla on vielä paljon tekemistä. Eri aikoina kehitetyt tietokannat ovat vailla riittävää yhtenäisyyttä. Tärkeä askel eteenpäin otettiin kuitenkin kesällä 2007, kun julkistettiin ajantasainen eli konsolidoitu säädöskokoelma 19 kielellä. Kun säädöskokoelma on osana EUR-Lex -tietokantaa, josta löytyvät myös perussopimukset, oikeuskäytäntö ja lainsäädännön valmisteluasiakirjat, se helpottaa eurooppalainsäädännön etsimistä. On kuitenkin huomattava, että kyseessä on EU:n julkaisutoimiston tuottama tietotuote, joka ei ole oikeudellisesti sitova.

Tärkeä oikeuslähdeopin muutos liittyy informaatio-oikeuteen. Informaation, sen käsittelyn ja siihen liittyvien oikeuksien merkitys on kasvanut olennaisesti, kun on siirrytty verkkoyhteiskuntaan. Informaatio-oikeudesta voidaan puhua erillisenä oikeusinformatiikkaan liittyvänä tai lainsäädännön määrän lisääntyessä jopa erillisenä oikeudenalana.

Informaatio-oikeuden keskeisinä periaatteina ovat informaation ja sen kulun vapaus. Lainvalmistelussa ja käytännöissä ahkeroivat kuitenkin eri intressitahot tekijänoikeusjärjestöistä suuryrityksiin. Vain yksi on yleensä poissa: kansalainen informaation kohteena, tarvitsijana ja käsittelijänä. Osin näistä syistä, kansalaisten edunvalvojiksi ja keskustelun käynnistäjiksi on syntynyt erilaisia asiantuntija- ja kansalaisjärjestöjä.

Kansainvälisillä asiantuntijajärjestöillä on oma paikkansa oikeuslähdeopin sallittujen oikeuslähteiden joukossa. Niiden tuottamalla tiedolla on oikeuslähdeopillista merkitystä ja sitä on syytä seurata tutkimuksen ja eri alojen kehityksen kannalta. Esimerkkejä kansainvälisistä asiantuntija- järjestöistä ovat henkilötietojen suojaan liittyen Privacy International ja Electronic Privacy Information Center (EPIC) sekä tekijänoikeuksiin liittyen Electronic Frontier Foundation (EFF). Järjestöissä on laajaa asiantuntemusta ja niissä seurataan tiiviisti kyseessä olevan alan kehitystä.

Suomessa ei toistaiseksi ole ylletty asiantuntijajärjestöjen tasolle näillä sektoreilla, vaan elämme lähinnä kansalaisjärjestöjen aikaa. Kansalaisjärjestöjen informaatiotakin on kansalaisyhteiskunnassa syytä seurata, vaikka samalla perustellusti epäillen.

Web 2.0 ja yhteisöllinen tiedontuotanto

Vuodesta 2003 lähtien verkkoympäristössä on tullut iskusanaksi Web 2.0. Sanotaan, että elämme uutta verkkoaikaa. Pinnallisimmin Web 2.0 on vain hyvin edennyt markkinointi-ilmiö.

Web 2.0 on toki enemmän. Kimmo Tuominen huomauttaa osuvasti, että Web 2.0 merkitsee yleensä tiedon tuottamista yhä enemmän käyttäjien toimesta. Käyttäjien erilaiset arviot, listaukset ja blogit tekevät verkosta entistä dynaamisemman tietoympäristön.

Web 2.0 aikakausi tuo parhaimmillaan uudenlaista yhteisöllisyyttä viestintään. Se sallii markkinavoimista vapaan viestinnän. Kysymys on samankaltaisesta laajamittaisesta muutoksesta, jota muutaman vuoden takainen Napster -tiedostojenjakelupalvelu tarjosi. Se toimi harrastelevien taiteilijoiden markkinointiverkostona, mutta siitä muodostui nopeasti myös laaja laittoman kopioinnin vertaisverkosto.

Web 2.0 on kuitenkin kokenut toisensuuntaisen muutosliikkeen. Markkinat ovat kiinnostuneet siitä. Moni suosittu sivusto on siirtynyt kaupallisen toimijan haltuun. Matka idealismista markkinoille on joskus lyhyt.

Miten oikeudellinen tieto sitten löytyy Web 2.0 -palveluista? Näkyvä ilmiö on tutkijoiden osittainen siirtymä staattisilta kotisivuilta dynaamisten blogien pitäjiksi. Blogeista on tullut tapa markkinoida ajatuksiaan ja tehdä itseään näkyväksi. Blogien lisäarvona kotisivuihin nähden ovat lukijoiden kommentit ja keskustelu heidän kanssaan.

Verkkoyhteisöllisyys on luontevaa ja hyväksyttävää. Medioissa on monia viestintää rajoittavia käytäntöjä. Niiden ei tulisikaan olla ainoita välineitä, joiden kautta tarjotaan ajankohtaista tietoa ja saadaan julkisuutta. Verkkosivut ja blogit ovat tiedon tiellä, myös tieteellisen ja mielipidetiedon osalta, tärkeitä vapaan tiedonvälityksen ja vaikuttamisen välineitä.

Parviälyä vai omatekoista asiantuntijuutta?

Tiedon käyttäjän kannalta tiedon arviointi on kasvava ongelma – löydetyn tiedon suhde ns. vallitsevaan käsitykseen on vaikeammin selvitettävissä. Vakavasti otettava, näennäistieteellinen ja julkisuushakuinen narsistinen tieto lähentyvät toisiaan. Hannu Lauerma toteaa osuvasti, että ”omatekoinen asiantuntijuus, joka saa julkisuutta Internetin ja kritiikittömien viikkojulkaisujen kautta, ei ole vaikeaa kehittää.”

Hiljattain on julkistettu ensimmäinen kotimainen oikeudellinen verk-

kotietosanakirja eli wikipedia: Lakiwiki. Se on tavanomaisesta poikkeava wikipedia siksi, että sen on tuottanut kaupallinen kustantaja. Julkaisun ilmoitetaan kuitenkin olevan kaikille vapaassa käytössä. Käyttäjät voivat myös muokata Lakiwikin tekstejä.

Lakiwikille oli sosiaalinen tilaus. Korkeatasoinen oikeudellinen sanakirjamme, Encyclopaedia Juridica Fennica, ei ole siirtynyt verkkoaikaan, eikä edes päivittynyt. Tuo Suomalaisen Lakimiesyhdistyksen toimesta syntynyt ja opetusministeriön rahoittamana valmistunut, mutta sittemmin kaupalliselle kustantajalle siirtynyt teos on esimerkki tiedon talouden ja tiedon tarpeen ristiriidasta. Sen korvaajaksi Lakiwikistä tuskin on.

Vasta tulevaisuus näyttää, miten kattava, luotettava ja koulukuntainen Lakiwikistä tulee yhtenäisten laatuvaatimusten puuttuessa. Oikeusvaltion näkökulmasta on toisaalta erikoista se, että Lakiwikistä on uutisoitu Finlexin avaussivulla. Viranomaisviestinnän neutraliteettivaatimus tuskin täyttyy silloin.

Oikeuskirjallisuus on jo ennen Web 2.0:n aikaa alkanut siirtyä ilmaisen verkkojakelun hyödyntäjäksi. Selkeimmin tämä on näkynyt sähköisten aikakausjulkaisujen alueella.

Etenkin Yhdysvalloissa osa merkittävistäkin oikeudellisista aikakauslehdistä ilmestyy verkossa joko sellaisenaan tai muutaman numeron viiveellä. Lisäksi open access -julkaisuissa on jonkin verran oikeudellisia julkaisuja. Lundin yliopiston kirjaston ylläpitämässä DOAJ luettelossa oli maaliskuun alussa 2008 jo 56 oikeudellista aikakauslehteä.

Verkkoyhteisöt ovat tuttuja jo varhaisilta verkon keskusteluryhmien ajoilta, vaikka Web 2.0 painottaa verkkoyhteisöllisyyttä. Niissä käydyllä keskustelulla on oma merkityksensä myös oikeudellista tietoa ajatellen. On valitettavaa, että suosituimmissa verkkoyhteisöissä keskustelun taso ja oikeudellisen tiedon asiantuntemus jäävät usein heikoksi.

Esimerkiksi keskustelut tekijänoikeuksista paljastavat kuitenkin asenteita, joilla voi - myönteisessä ja kielteisessä mielessä – olla vaikutusta lainvalmisteluun tai jopa poliisin toimintaan. Avoin verkkokeskustelu antaa perinteisen median mielipidepalstoja luontevamman ja vapaamman pohjan yhteisölliselle tiedonmuodostukselle sekä kansallisilla että kansainvälisillä foorumeilla. Puhutaan jopa parviälystä, jolloin käyttäjät ikään kuin verkostoitumisen sivutuotteena rakentaisivat joukkovoimaa tai yhteisöllistä ajattelua.

Toisaalta ei tulisi unohtaa oikeudellisen tiedon arvokkuutta ja siihen liittyviä laatuvaatimuksia. Yhteisöllinen keskustelu oikeasta ja oikeu-

desta on usein jännitteisessä suhteessa laadukkaampiin oikeudellisen tiedon ympäristöihin. Mielipiteet oikeasta ja sen ilmaisutavat vaihtelevat olennaisesti.

Matti L. Ahon tunnettua lausumaa mukaillen oikeus on kuin tasku, mihin itse kukin laittaa haluamansa sisällön. Verkkokeskustelu näyttää suurentavan tuota taskua aika lailla. Kansalaisen olisi osattava erottaa, mikä tieto on mistäkin lähteestä.

Tieto etääntyy käyttäjästä

Tietoverkon väitetään usein tuovan tiedon lähemmäs käyttäjää. Tämä pitää epäilemättä paikkansa silloin, kun tiedämme, mitä tietoa olemme hakemassa ja missä sitä on saatavilla. Finlex on vajavuuksistaan huolimatta hyvä esimerkki informaation lähentymisestä. Myös Ruotsin Lagrummet on viime vuosien uudistumisen myötä muotoutunut keskeiseksi virallisen oikeudellisen tiedon perustietovarannoksi. Se palvelee varsin hyvin myös suomalaisia tarpeita ja on kattavuudessaan ajanut jopa Finlexin ohitse.

Oikeudellisen tiedon käytön kannalta tiedonhaulla on kriittinen merkitys, kuten oikeusinformatiikan pohjoismainen uranuurtaja Peter Seipel asian toteaa. Vain harvoin tiedämme ennalta riittävästi, jotta voisimme hakea oikeaa tietoa. Yleensä tarvitsemme uutta informaatiota uuden tiedon muodostamiseksi tai vanhan tukemiseksi.

Jos oikeudellinen perustietovaranto on hyvätasoinen, verkko tuo keskeisen virallisen oikeuslähdeaineiston lähemmäksi lakimiehiä ja kansalaisia. Tiedon käyttö edellyttää kuitenkin osaamista sen arvioinnissa. Muutoin olemme hyvin helposti ns. Google-sivistymättömyyden vankeja - luulemme löytäneemme tiedon, vaikka sen oikeellisuudesta ja lähteistä ei välttämättä olisi takeita.

Tiedonhaku edellyttää myös sisältöjen ja tiedonhaun menetelmien tuntemusta. Avoin tietoverkko ja hakukone muodostavat usein hedelmättömän yhdistelmän etsittäessä oikeustieteellistä aineistoa, etenkin kansainvälistä aineistoa, ilman riittävää alakohtaista asiantuntemusta. Olisi osattava valita oikeat tiedonlähteet ja hakusanat sekä tunnettava, miten asiasta puhutaan oikeuden kielessä.

Kehittynyt oikeudellinen tiedonhaku avoimissa tietoverkoissa edellyttää oikeudellista asiantuntemusta, laadukkaiden tiedonlähteiden tuntemusta ja tietopalvelun ammattilaisten apua ns. harmaalla alueella liikuttaessa. Silloinkin on osattava varoa aineistoa, jolla ei ole oikeus-

lähdearvoa, kuten yhden asian kansalaisjärjestöjen, konsulttien tai maallikoiden sivustoja. Kaikkia niitä löytyy.

Oikeudellinen tiedon keskittyminen tietyille osapuolille on myös ongelmallista. Tätä kirjoitettaessa kehitteillä on tuomariportaali. Se tarjoaisi tuomareille näiden tarvitsemaa oikeudellista aineistoa. Ajatus on kiintoisa, mutta oikeusvaltion näkökulmasta vaarallinen. Jos, kuten on todennäköistä, tuollainen portaali kaventaisi tuomarin tiedonhakua vain tiettyihin aineistoihin, se olisi vastoin oikeuslähdeoppiamme. Ja jos se olisi vain tuomarikunnan käytössä, se muuttaisi osapuolten informaatiotasapainoa oikeudenkäynneissä. Kokonaisuutena yhdistelmä tuomarin lakikirja – sellainen on jo olemassa – ja oikeudellisen tiedon tuomariportaali saattaa ylittää demokratian sallitut rajat.

Oman oikeudellisen etääntymisen ongelmansa tuottavat erilaiset julkisen sektorin ohjeistukset. Viranomaisen velvollisuus viestintään on tuottanut mittavan määrän kotisivuja ohjeineen. Ongelma on kuitenkin siinä, miten voimallinen tai löyhä suhde lainsäädäntöön näillä ohjeilla on. Huonon byrokratian yksi tunnusmerkki on se, että ohjeet alkavat elää laista riippumatonta elämää.

Viestintävelvollisuuden synnyttämistä ohjeista on erotettava ne ohjeet, mitä viranomaiset oman ohjausvelvollisuutensa puitteissa tarjoavat. Esimerkiksi tietosuojavaltuutetun nimenomaisena velvollisuutena on ohjata tietosuojakäytäntöjä. Tämän vuoksi tietosuojavaltuutetun toimiston sivustolla on tavanomaista painavampi oikeudellinen merkitys.

Laadukas tieto, hakutaidot ja laintulkinta avaimina demokratiaan

Oikeudellisen tiedon kehitys verkkoyhteiskunnassa näyttää edelleen olevan kulkemassa neljään erilaiseen ja osin toisistaan poikkeavaan suuntaan. Avoimet tietoverkot eivät sellaisenaan ole yksiselitteinen avain oikeudellisen tiedon hallintaan.

Ensinnäkin, jos arvostetaan hyvää tiedonhallintaa, tarvitaan avoimen tietoverkon ilmaisaineistojen lisäksi maksullisia oikeudellisia tietokantoja, mutta myös muita maksullisia tietotuotteita ja hyviä tiedonhakuvalmiuksia verkkoaineistosta. Tieto maksaa vastakin ja tiedonhaku sekä tiedon hankinta ovat edelleen taitoa vaativia toimia.

Tiedon arvoketju matkalla halvasta ja helposti tavoitettavasta tiedosta laadukkaiksi ammatillisiksi tietotuotteiksi on monipolvinen ja erilaisia ammattitaitoja edellyttävä. Näin kehittyvät organisaatiokohtaiset kalliit

tietoympäristöt, joiden piirissä ovat esimerkiksi suuret asianajotoimistot, tuomioistuimet ja yliopistot. Näissä tietoympäristöissä on tyypillisesti käytössä laajat sisäiset tietovarannot, kuten Intranetin kautta saatavilla olevat julkaisurekisterit ja asiakirjat. Tietovarantoja täydentävät myös monipuoliset maksulliset aineistot, kuten artikkelitietokannat tai lehtiarkistot, jotka saattavat olla vain talon sisäisessä käytössä tai tarjolla niille, jotka tulevat käyttämään aineistoja paikan päälle.

Hyvän tietojohtamisen myötä organisaatioihin voi kehittyä tärkeitä työtä tukevia oikeudellisia tietovarantoja ja niiden sisältöä ja käyttöä hallitsevia ja oikeudellisen asiantuntemuksen omaavia vastuuhenkilöitä. Tämä toisaalta tuo informaatioepätasapainoa suhteessa niihin, joilla ei vastaavia resursseja ole.

Kansallisen elektronisen kirjastomme, FinElibin, ja siinä mukana olevien tieteellisten ja yleisten kirjastojen etuna on se, että niiden moninaiset ja monialaiset tietokannat ylittävät ahtaat tieteenalarajat. Hyvä tiede ja hyvä tiedonhaku ovat yhä useammin monitieteisiä. Esimerkiksi yksityisyys ja tietosuoja ovat aihepiirejä, joilla on välttämätön yhteys sosiologiaan, filosofiaan ja tietojenkäsittelytieteeseen. Esimerkiksi Amitai Etzionin teos Limits of Privacy, SpringerLinkin lukuisat eri alojen aikakauslehdet ja toisaalta tieteellinen tietokanta Scirus ovat noiden aihepiirien pohtijalle välttämättömiä aineistoja.

Kansalaisten tiedon tarve verkkoyhteiskunnassa on myös huomioitu kiintoisalla tavalla FinElibin toimesta. Sen puitteissa on osana yleisempää tiedonsaannin edistämistä käynnistynyt hanke saada rahoitusta keskitetyille, verkon kautta käytettäville sähköisille perustietovarannoille. Tällaisten työelämän, koulutuksen ja vapaa-ajan tietoaineistojen joukkoon kuuluu myös oikeudellista aineistoa. Ongelmallista on kuitenkin, ettei aineistoa välttämättä ole valmiina ja sitä olisi tuotettava.

Oikeudellisen tiedon alueella mahdollisuuden tähän tarjoaisi uudenlainen käsitys lainsäädännöstä – sähköinen interaktiivinen lainsäädäntö. Sellaisia olisivat säännösperusteiset tuotteet, joissa säännöstekstit yhdistyisivät tausta-aineistoihin – “mikä” ja “miksi” olisivat yhtä lailla näkyvillä. Lakitekstin ymmärtäminen on tärkeä osa toimivaa demokratiaa. Matkalla parempaa lainvalmisteluun tällä tavalla interaktiivinen lainsäädäntö olisi olennainen laatutekijä.

Kolmas havainto liittyy verkon demokraattisuuteen. Avoimen tietoverkon on monesti väitetty olevan askel kohden demokratiaa. Sananvapaus yksilön vapautena on toteutettavissa entistä helpommin. Verkko tarjoaa kuitenkin erinomaisen alustan sellaiselle verkostoitumiselle,

missä myös tiedon oikeellisuus samalla vaarantuu aikaisempaa enemmän. Informaatiota muunnetaan. Jos laatujärjestelmät sivuutetaan tiedon tuotannossa, liberalistisen lehdistöteorian vanha ajatus itse itseään korjaavasta totuudesta on ehkä entistäkin kauempana.

Toisaalta avoin verkko tukee verkostoitumista. Yhdysvalloissa on jo menestyksellä selvitetty oikeudellisten vaikuttajien aikaansaamaa verkostoitumista. Paul Erdõsin tunnuslukuajatus, jonka mukaan kuka tahansa kytkeytyy kehen tahansa toiseen henkilöön maailmassa maksimissaan kuuden tuttavan ja hänen tuttaviensa kautta, kuvaa hyvin verkostoitumisen mahdollisuuksia. Tästä kehitetty iskulause ”six degrees of separation” on tukenut myös oikeudellisen informaation ja kulttuurin tutkimusta. Se tuo muutoin näkymättömän verkostoitumisen merkityksen näkyväksi.

Kirjastojen käyttöä yleisesti ja tutkimuksen tekoa erityisesti koskee viimein neljäs kehityssuunta. Jon Bing on sattuvasti todennut, että etsiessämme tiettyä kirjaa kirjastosta, tiedämme jo sen olemassaolon. Mutta seuraava kirja, jota emme vielä tunne, saattaa olla myös tärkeä – kenties vielä tärkeämpi.

Kirjastoissa paikan päällä tapahtuva, osin satunnainen samoilu ja selailu, on käyttäjille hyvin olennainen tapa tehdä löytöjä. Se näyttäisi kuitenkin olevan vähenemässä verkkoaineistojen käytön lisääntymisen myötä, jonka keväällä 2007 tehty FinElibin käyttäjätutkimus hiljattain vahvisti. Se on sivistyksen kannalta huolestuttavaa.

Kansalaisen oikeudet tiedon valtatiellä

Ahti Saarenpää

Yksi vaikeimmista asioista elämismaailmassamme on nykyisin sen tunnistaminen, millaisessa yhteiskunnassa kulloinkin elämme. Aiemmin se oli helpompaa. Saatoimme puhua maatalousyhteiskunnasta tai teollisesta yhteiskunnasta ja havaitsimme asiaa enemmän pohtimatta elävämme niissä.

Tänään tilanne on toinen. Yhteiskunnan nopeat muutokset ja monimuotoistuminen vaikeuttavat ymmärtämistä. Erilaisten tuotteiden ja palvelujen massat ympäröivät jokapäiväistä elämäämme. Yhteiskuntaa on vaikea tunnistaa.

Viestintä puolestaan tuo matkassaan kilpailevia näkökulmia ja nimikkeitä. Yksi niistä on tietoyhteiskunta. Emme voi välttyä tuon sanan näkemisestä ja kuulemisesta.

Tietoyhteiskunnasta verkkoyhteiskuntaan

Tietoyhteiskunta -termillä on monia merkityksiä. Peter F. Drucker ei ehkä osannut 1960-luvun lopulla tietoyhteiskunnasta (knowledge society) puhuessaan ennakoida sitä, että nykyisin suorastaan hoemme Suomessa samaa sanaa, mutta toisessa merkityksessä. Se on löytänyt sijansa jopa valtioneuvoston politiikkaohjelmiin. Kansallinen tietoyhteiskuntastrategia tähtää jo vuoteen 2015.

Tietoyhteiskunta on sanana ollut pitkään sekä käännösvirhe että ajatusvirhe. Suomessa puhutaan tietoyhteiskunnasta, kun muualla yleensä ilmaisuna on informaatioyhteiskunta.

Keskustelua aidon tietoyhteiskunnan mahdollisuudestakin käydään. Silloin tietoyhteiskunnalla tarkoitetaan kuitenkin tämänpäiväisestä paljon pidemmälle kehitettyä, informaation nykyistä älykkäämmälle käsittelylle rakennettua yhteiskuntaa. Siihen on vielä matkaa, mutta esimerkiksi radiotaajuisen tunnistamisen (RFID) nopeasti yleistyvä käyttöönotto antaa jonkin verran aikaisempaa paremman perustan puhua tietoyhteiskunnasta. Arjen tietoyhteiskunta on siihen liittyvä uusi ilmaisu.

Toki myös EU:n sivustoilta löydämme nykyisin tietoyhteiskunta -sivuston (knowledge society), joka on osana työllisyys- sosiaali- ja tasa-arvoasiain sivustoa! Ja omassa yleisessä suomalaisessa asiasanastossamme (YSE) tietoyhteiskunnan sanotaan käsitteenä korvaavan informaatioyhteiskunnan.

Jo alkuvaiheen informaatioyhteiskunnassa informaatiolla ja sen käsittelyllä on ollut keskeinen merkitys. Olemmehan useimmilla aloilla toimineet jo vuosikymmeniä merkittävässä määrin tietojärjestelmien varassa. Tietotekniikka on tullut arkipäivään.

Yhteiskunnan kehityksessä seuraava askel informaatioyhteiskunnasta eteenpäin on ollut verkkoyhteiskunta. Se merkittävä rakenteellinen yhteiskunnallinen muutos, mitä olemme viime vuodet todistaneet, liittyy juuri tietoverkkoihin. Toimintaympäristömme on saanut uuden yleisen informaatioinfrastruktuurin. Yhteiskunnan toiminnot ja asiointi rakentuvat laajalti verkkojen varaan.

Verkkoyhteiskunnan käsitettä pohjustivat jo 1970-luvulle tultaessa James Martin ja Osmo A. Wiio. Sen liittäminen, kuten toisinaan näkee tehtävän, Manuel Castellsin myöhemmin näkyvästi markkinoimaan verkostoajatteluun on selkeä ajallinen ja aatteellinen erhe. Verkot ja verkostot ovat eri asioita.

Huomio on, kuten Jan van Dijk viittaa, kiinnitettävä ensisijaisesti infrastruktuurin. Infrastruktuurilla tarkoitetaan yleisesti sitä järjestelmää, jonka varaan yhteiskunnallisesti merkittävät toiminnot, palvelut ja väylästöt rakentuvat.

Uuden infrastruktuurin vaikutukset

Infrastruktuureille on tyypillistä niiden jokapäiväisyys ja helppokäyttöisyys. Infrastruktuureja ovat niin luonteva osa yhteiskunnassa ja arjessa toimimista, että niiden merkitykseen havahdutaan vasta poikkeavissa tilanteissa. Poikkeustilanteiden yhteydessä puhutaan kriittisistä infrastruktuureista, joiden toimimattomuus vaarantaa yhteiskunnan keskeisiä toimintoja.

Infrastruktuurin käsitettä käytetään tietoteknologian kielessä usein suppeammassa merkityksessä kuvaamaan jonkin toiminnan perusrakennetta. Tyypillisiä tällaisia ilmaisuja ovat julkisen avaimen infrastruktuuri (PKI) puhuttaessa sähköisistä allekirjoituksista tai paikkatietojärjestelmän infrastruktuuri. Puhe on tuolloin vain yleisemmän informaatioinfrastruktuurin yksittäisestä osasta. Niillä voi kuitenkin olla omat oikeudelliset viitekehyksensä.

Verkkoyhteiskunnassa on merkitystä sekä passiivisella eli erilaisissa tietovarastoissa saatavilla olevalla informaatiolla, mutta myös informaation aktiivisella tarjonnalla ja käytöllä. Lisäksi medioiden verkkoviestinnän rinnalle on tullut välitön ja vuorovaikutteinen kansalaisviestintä verkoissa. Perinteisen median siirtyminen myös verkkoon kertoo verkkoviestinnän mahdollisuuksista, mutta myös median valta-aseman heikentymisestä. Viestintä on entistä monimuotoisempaa ja osin vapaampaa.

Tietoyhteiskunnan infrastruktuuri tarjoaa verkostoitumiselle erilaisia uusia mahdollisuuksia. Monilla niistä on merkitystä myös oikeudellisen tiedon välityksessä. Näistä esimerkkeinä ovat maahanmuuttajien tai muiden vähemmistöjen rajat ylittävät verkkoyhteisöt.

Virtuaaliyhteisöt tuovat mukanaan myös uusia viestinnällisiä ja oikeudellisia haasteita. Kulttuurin tasosta, tai tasottomuudesta kertovat omaa kieltään Facebookin tapaisten yhteisöjen menestystarinat. Niistä on muodostunut laaja-alaisia yksityisten kertomusten kokoelmia, mutta myös poliittisen tiedonvälityksen kanavia. Turhaan eivät Euroopan tietoturvavirasto (ENISA) ja tietosuojavaltuutetun toimisto olekaan julkaisseet ohjeitaan yksityisyyden suojaamisesta uusissa verkkoyhteisöissä.

Uuden informaatioinfrastruktuurin vaikutuksiin ollaan heräämässä. Näkyvänä herättelijä on ollut Euroopan Unioni, jonka viime vuosien politiikkaohjelmat rakentuvatkin tietoverkkojen tehokkaan ja monipuolisen hyödyntämisen ajatukselle.

Viimeisimpänä esimerkkinä on i2010, kasvua ja työllisyyttä edistävä eurooppalainen tietoyhteiskuntaohjelma. Eri toiminnot opetuksesta terveydenhuoltoon ja hallinnosta markkinoihin halutaan muuntaa merkittävässä määrin tietoverkoissa toimiviksi. Siinä on verkkoyhteiskunnan ydin – tulemme riippuvaisiksi verkoista.

Suomalaisen esimerkin tietoverkkojen laajamittaisesta hyödyntämisestä tarjoaa myös sosiaali- ja terveydenhuollon valtakunnallisten tietojärjestelmäpalvelukuiden perustaminen. Verraten vähälle huomiolle jäänyt hanke tuo potilastiedot yhdenmukaisesti verkkoihin. Sen toteutuminen testaa aikanaan hyvin myös yksityisyytemme suojaa massiivisten tietojärjestelmien puitteissa.

Lainsäädäntö ja infrastruktuuri

Verkkoyhteiskunnan informaatioinfrastruktuurin vaikutukset kohdistuvat myös lainsäädäntöön ja sen soveltamiseen. Euroopan Unionin lainsäädäntöä on vähitellen kehitetty verkot huomioon ottavaksi. Legal framework eli oikeudellinen viitekehys on toistuva ilmaisu eurooppalaista verkkoyhteiskuntaa rakennettaessa.

Suomessa varsin merkittävä, mutta julkisuudessa vähälle huomiolle jäänyt edistysaskel otettiin korkeimman hallinto-oikeuden ennakkoratkaisussa KHO:2006:18. Siinä korkein hallinto-oikeus oikeutti vammaisen henkilön saamaan itselleen muuttuneen teknologian mukaiset ruudunluku- ja puhesynteesiohjelmat.

Tuomion perusteluissa todettiin seuraavaa: “Kun otetaan huomioon julkisten ja yksityisten palvelujen alati laajeneva siirtyminen ensisijaisesti verkon kautta käytettäviksi, A:n apuvälineissä ei ole kysymys harrastustoiminnan tukemisesta vaan sosiaalisen toimintakyvyn tukemisesta sekä itsenäisen elämäntilanteen hallinnan ja päivittäisistä toiminnoista selviämisen. edistämisestä”.

Lausuma on selkeä kannanotto yksilön oikeuksien ja yhdenvertaisuuden puolesta verkkoyhteiskunnassa. Vammaisuus ei saa olla esteenä verkkoon pääsylle silloin, kun verkko on yleinen informaatioinfrastruktuuri. Muutoin toteutuisi kansainvälisessä keskustelussa paljon huomiota saanutta digitaalinen tietokuilu (digital divide) tietotekniikan hyödyntäjien ja näiden mahdollisuuksien ulkopuolelle jäävien välillä.

Infrastruktuuri vaikuttaa yksilön asemaan yhteiskunnassa. Informaation monimuotoisuus, sen uudet käyttötavat ja uudet viestintätilanteet tuovat uudenlaisia haasteita. Uusia kysymyksiä ovat myös, millä tavoin ja millaisin edellytyksin aidossa demokratiassa kansalainen viestii, etsii tietoa, käy kauppaa, käyttää palveluja, päättää omista asioistaan tai vaikuttaa yhteiskunnan asioihin tietoverkkoja hyödyntäen.

Kysymyksillä on vanha historiallinen taustansa, johon verkkoyhteiskunnan oikeus perustuu. Hyvän esimerkin tarjoaa korkeimman oikeuden ennakkoratkaisu KKO:2007:6. Siinä luottokorttiyhtiö asetettiin vastuuseen siitä, että sen hyväksymä ulkomainen yhtiö ei ollut verkkokaupassa täyttänyt toimitusvelvollisuuttaan. Tämä aiempien lainvalmistelutöiden valossa laventava tulkinta voidaan perustellusti nähdä kuluttajaa suojaavana verkkoyhteiskunnan tulkintana.

Demokraattinen oikeusvaltio ja kansalaisen perusoikeudet

Yhteiskuntaa ja sen sääntelyä ei voi arvioida ottamatta huomioon valtiota. Demokratian kehityksessä olemme edenneet demokraattisen oikeusvaltion asteelle. Demokratiahan olemme muodollisesti olleet koko itsenäisyyden ajan.

Oikeusvaltio on käsitteenä jo vanha, mutta sen merkitys on jäänyt melko epäselväksi. Usein sillä viitataan viranomaisen velvollisuuteen noudattaa lakia sekä oikeudenmukaiseen oikeudenkäyntiin. Tämä menettelyllinen ns. rule of law -periaate on yksi merkittävä osa oikeusvaltion ajatusta. Se ei kuitenkaan ole ainoa, eikä edes merkittävin oikeusvaltion tunnusmerkki.

Eurooppalaisen oikeusvaltion perusajatuksena on ihmisen ja hänen perusoikeuksiensa kunnioittaminen. Ilmaisu “constitutional state” eli perustuslaillinen oikeusvaltio kuvaakin paremmin oikeusvaltiota. Se on sekä materiaalinen että menettelyllinen oikeusvaltio. Tätä käsitteiden erottelua käytetään nykyisin esimerkiksi Unescon demokratiasta kertovilla, tärkeillä Dadalos -opetussivuilla.

Ihmisen ja hänen oikeuksiensa aikaisempaa laajempi ja tehokkaampi kunnioittaminen oikeusvaltion lähtökohtana on johtanut ja johtamassa kolmeen olennaiseen muutokseen oikeudellisessa sääntelyssä ja sen tulkinnoissa.

Ensinnäkin (1) yksilön itsemääräämisoikeus on säädetty entistä laajemmaksi suhteessa valtioon, eri organisaatioihin ja kanssaihmisiin. Aikaisempi hallintovaltio oli pahimmillaan ihmistä alistava valtio. Olimme sanan varsinaisessa merkityksessä hallintoalamaisia. Oikeusvaltiossa hallinnon tulisi olla ihmistä varten.

Toiseksi (2) yksilön oikeuksista ja niiden rajoituksista säädetään yhä enemmän lailla. Lakisääteisyys lisääntyy. Esimerkiksi viranomaisen yleistoimivalta on jo väistynyt ajattelumalli. Jopa erilaisista suljetuissa laitoksissa perinteinen pakkovalta on väistynyt yksityiskohtaisen sääntelyn tieltä. Samalla säädösten ja säännösten määrä lisääntyy.

Ja kolmanneksi (3) lainsäädäntömme nivotaan entistä tiukemmin ihmis- ja perusoikeuksiin. Jokainen yksittäinen säännös ja sen tulkinta kytkeytyy myös ihmis- ja perusoikeuksiin ja niiden määritelmiin siitä, mikä kulloinkin on oikein. Voimme nykyisen perustuslain myötä myös perustellusti puhua perusoikeusvelvoitteisesta laintulkinnasta.

Oikeusvaltio ja verkkoyhteiskunta

Oikeusvaltioksi on tultu vähitellen. Oikeusvaltioperiaate on nykyisin vahvistettu perustuslain 2 §:ssä. Tuon kehityksen edistäminen on myös oikeusministeriön oikeuspolitiikan strategian lähtökohta sekä yksi ministeriön hallinnonalan kansainvälisistä tavoitteista.

Oikeusvaltion ja verkkoyhteiskunnan liki yhtäaikainen kehitys on meillä sattuman tulosta. Näkyvä oikeusvaltioon siirtyminen alkoi ulkopoliittista syistä 1990-luvun alussa Suomen voidessa tuolloin liittyä Euroopan neuvostoon ja Euroopan ihmisoikeussopimukseen.

Aiemmin olimme olleet piilevästi oikeusvaltio, sillä sana ei kuulunut oikeudellisen elämän perussanastoon. Liittyminen Euroopan unioniin vahvisti edelleen oikeusvaltiokehitystä, sillä EU:n johtavana oikeusperiaatteena on ihmisoikeuksien kunnioitus. Tätä harvemmin muistetaan ihmeteltäessä asetusten ja direktiivien määrää.

Verkkoyhteiskunta alkoi konkretisoitua tietoteknisen kehityksen myötä 1990-luvun puolessa välissä. Avointen tietoverkkojen käyttöönotto ja teknologinen konvergenssi eli erilaisia toiminnallisuuksia yhdistävien teknologioiden sopeutuminen samoihin verkkoihin ovat avanneet tietä nykyiseen verkkoyhteiskuntaan. Teknologista konvergenssia seuraa vähitellen myös oikeudellinen konvergenssi. Se näkyy monin tavoin lainsäädännön uudistuksissa ja uudessa lainsäädännössä.

Oikeuden kieleen oikeusvaltio on tullut hitaasti. Perustuslain ohella oikeusvaltiosta puhutaan merkittävästi vain laissa sanavapauden käyttämisestä joukkoviestinnässä. Tuo vuodelta 2003 oleva uusi laki, jonka monimutkainen nimi edustaa perin vanhanaikaista säätämistekniikkaa, on verkkoyhteiskunnan sananvapauslaki. Se on tarkasti ottaen yksi useammasta sananvapauteen vaikuttavasta laista.

Sananvapauslaissa asetetaan ihmisoikeussopimusten mukaisesti sananvapauden rajoittamisen edellytykseksi välttämättömyys. Viestintään ei ole lupa puuttua “enempää kuin on välttämätöntä ottaen huomioon sananvapauden merkitys kansanvaltaisessa oikeusvaltiossa”.

Oikeusvaltio on myös oikeuskäytännössä harvoin mainittu käsite. Ylimpien tuomioistuintemme ennakkoratkaisuissa se ilmenee vain muutaman kerran ja silloinkin tyypillisesti korkeimman oikeuden eriävissä mielipiteissä.

Oikeuskirjallisuudessa oikeusvaltio sitä vastoin on terminä jo jonkin verran yleisemmässä käytössä. Esimerkiksi oikeuspoliittisessa keskustelussa oikeusvaltio on iskusana, jonka tyypillistä käyttöä ovat luonnehdinnat, minkä mukaan jokin asia ei ole oikeusvaltion ajatuksen mukai-

nen. Käsitteen tuollainen käyttö näkyy myös sen varhaisen synnyinmaan Saksan verkkokeskusteluissa.

Kaiken edellä mainitun seurauksena on oikeuden aikaistuminen. Suhteessa julkiseen valtaan ja muihin kansalaisiin meillä on oikeus odottaa oikeuksiamme kunnioitettavan mahdollisimman aikaisessa vaiheessa eri toimia ja toimintaprosesseja. Sama koskee myös oikeuden ja tietotekniikan suhdetta verkkoyhteiskunnassa. Tuossa oikeusinformatiikan alaan kuuluvassa tarkastelussa ajatus oikeusvaltiosta on väistämätön osatekijä.

Tietotekniikka ja oikeudellinen tutkimus

Teknologian kehitys on muidenkin kuin teknisten tieteiden tutkimuskohde. Tuskin missään tieteessä voidaan sitä enää sivuuttaa. Historian tutkimuksessakin tarkastellaan jo tietotekniikan historiaa.

Akateemikko Georg Henrik von Wrightin pohdinnat teknologian hyödyntämisen ongelmista ovat osoittaneet, miten tärkeää teknologian kehitystä on arvioida myös filosofin silmin. Teknologinen imperatiivi eli usko teknisen kehityksen kaikkivoipaan myönteisyyteen on yhä kasvava riski yhteiskunnan kehitykselle. Erilaiset tietoyhteiskuntastrategiat ja niiden markkinointi ovat tästä hyviä esimerkkejä.

Oikeuden ja teknologian suhde on myös oikeuden yleistieteiden tasolla ohittamaton kysymys. Mikään oikeudenala ei voi välttää teknologian kehityksen seuraamista osana yhteiskunnan kehitystä. Muutoin oikeustiede ei täyttäisi perustehtävänsä: yhteiskunnan palvelemista.

Etenkin Yhdysvalloissa onkin jo pitempään ilmestynyt oikeuden ja teknologian suhdetta tarkastelevia oikeudellisia aikakauslehtiä. Osa niistä on oikeustieteen lähtökohdista ponnistavia “law and technology” -otsakkeella toimivia. Osa painottuu tekniikan tutkimukseen “technology and law” -otsakkeella. Niille on lisääntyvässä määrin yhteistä riskien näkökulman esille ottaminen.

Olisi kuitenkin keinotekoista pyrkiä luomaan lainopin tasolla oppiaine nimeltä oikeus ja teknologia. Se liittäisi äärimuodoissaan yhteen asioita, jotka lainsäädäntöä silmällä pitäen olisivat yhteismitattomia. Esimerkiksi sähköntuotannon tehoreservien sääntelyn ja autojen ajovalojen tehokkuuden sääntelyn tutkiminen saman oppiaineen puitteissa olisi vastoin tieteen rationaalisuuden johtavaa ajatusta.

Oikeuden ja teknologian suhde on vanha ja teknologian kehityksen myötä hajanaisemmaksi käyvä aihepiiri. Oikeusinformatiikka sen sijaan

edustaa uudempaa ja yhtenäisempää oikeustieteellisen tutkimuksen ja opetuksen näkökulmaa. Siinä tutkitaan oikeuden, informaation ja tietotekniikan välisiä suhteita sekä niissä ilmeneviä oikeudellisia sääntely- ja tulkintakysymyksiä.

Oikeusinformatiikka

Modernia oikeusinformatiikkaa nivoo yhteen nykyaikaisen tietotekniikan kehityskulku. Tietotekniikka on sinänsä pieni, mutta yhteiskunnallisilta vaikutuksiltaan suuri ja jatkuvassa murroksessa oleva osa teknologian kehitystä. Oikeusinformatiikan alullepanijat osuivatkin aikanaan eräänlaiseen tieteelliseen kultasuoneen.

Oikeusinformatiikka tutki varhaisessa vaiheessaan, 1940- ja 1950-luvuilla, erityisesti tietotekniikan oikeudellisen hyödyntämisen mahdollisuuksia. Kysymys oli uuden apuvälineen löytämisestä. Tehtävä jatkuu edelleen, mutta nyt digitaalisessa toimintaympäristössä.

1960-luku ja etenkin 1970-luku toivat kuvaan mukaan uusia käytännön oikeuselämän ja oikeudellisen sääntelyn kannalta tärkeitä aihepiirejä. Esimerkiksi kysymys siitä, millaista oikeudellista suojaa tietokoneohjelmistojen tekijät voivat saada, tuli ajankohtaiseksi ohjelmistojen saadessa markkina-arvoa erikseen hyödynnettävinä tuotteina. Toimistoautomaation kehitys pakotti ottamaan kantaa esimerkiksi tietoturvallisuuteen. Ja tietosuojasta yksityisyyden suojana tuli laajan kansainvälinen keskustelun aihe jo 1960-luvun kuluessa.

Oikeusinformatiikka on nykyisin tapana jakaa yleiseen ja erityiseen osaan. Yleisen osan puitteissa tarkastellaan oikeudellisen verkkoyhteiskunnan kehitystä, informaatioinfrastruktuurin oikeudellista merkitystä, tietojärjestelmien käytön oikeudellisia reunaehtoja sekä lakimiesten tietoteknisiä valmiuksia.

Oikeusinformatiikan erityisessä osassa tarkastellaan lähemmin oikeudellista tietojenkäsittelyä, oikeudellista informaatiota, informaatio-oikeutta sekä tietotekniikkaoikeutta, jota kansainvälisesti myös kutsutaan nimellä IT-oikeus (information technology law). Monesti IT-oikeuden nimikkeen alla on myös informaatio-oikeutta.

Oikeusinformatiikan aihepiiri nykyisessä verkkoyhteiskunnassa on verrattain laaja. Matka esimerkiksi sähköisen hallinnon tutkimuksesta osana oikeudellista tietojenkäsittelyä oikeudellisen tiedonhaun tutkimukseen osana oikeudellisen informaation tutkimusta on pitkä. Sen myötä oikeusinformatiikkaan on tullut erikoistumista.

Oikeusinformatiikan muutos liittyy myös yhteiskunnan ja valtion muutokseen. Oikeudenalan synnytti kiinnostus tietotekniikan oikeudelliseen merkitykseen, mikä on edelleen yksi oikeusinformatiikan peruspilareista. Ulottuvathan kehittyvän tietotekniikan hyödyntämisen vaikutukset lakimiesten ammattitaidon ydinalueille. Yhtä lailla on edelleen tarpeen havahduttaa tietotekniikkaa vähemmän tunteva, jopa osin pelkäävä lakimieskunta verkkoyhteiskunnan oikeudellisiin ongelmiin.

Oikeusinformatiikan toinen peruspilari on ihmiskäsitys. Oikeusvaltion kehityksen myötä on tullut entistä tärkeämmäksi seurata ja arvioida yksilön oikeuksien toteutumista digitaalisessa ympäristössä. Tämäkin on ollut oikeusinformatiikalle tuttua jo pitkään. Esimerkiksi henkilötietojen käsittelyä ohjaava tietosuojalainsäädäntö on mitä syvimmin yksilön ja ihmiskäsityksen oikeutta. Uudessa informaatioinfrastruktuurissa aihe on entistä tärkeämpi, kun perusoikeuksiemme käyttö on siirtynyt suurelta osin verkkoihin ja oikeus yksityisyyteen on perusoikeuksista merkittävimpiä.

Yhteiskunnan kehityksen myötä oikeustiede on jakautunut yhä useampiin erityisalueisiin. Euroopassa tunnetaan jo ainakin 60 eri oikeudenalaa. Oikeusinformatiikka on vakiintunut yhdeksi niistä. Erikoistuminen on osin välttämätöntä, mutta samalla vaarallista. Systematiikka, etenkin vakiintunut systematiikka, avaa ja sulkee näkökulmia.

Oikeusinformatiikka on tieteenä epäilemättä erikoistumisen tulosta. Tietotekniikka ja informaatio ovat olleet systematisoinnin avaimia. Oikeusinformatiikka on kuitenkin myös yhdistävä ja yhteistyötä avaava tiede. Esimerkiksi tietosuojalainsäädäntö on oikeusinformatiikan ja persoonallisuusoikeuden yhteinen tutkimusalue. Toisin ei voisi ollakaan yksilön oikeuksista puhuttaessa.

Infrastruktuuri sääntelyn kohteena

Yhteiskunnan infrastruktuurien muutokset ovat asioita, joita lainsäätäjä ei saa olla huomaamatta. Esimerkiksi tieliikenteen säännöt syntyivät varsin pian autojen käyttöoton jälkeen. Vastaavasti teletoiminnasta tuli Euroopassa useimmissa maissa valtion ohjaamaa ja usein myös valtion harjoittamaa toimintaa. Suomi lukuisine toimilupalaitoksineen oli tässä suhteessa pitkään näkyvä poikkeus.

Verkkoyhteiskunnassa tietoverkot ovat nousseet muiden merkittävien infrastruktuurien rinnalle ja jopa niiden ohitse merkittävyydeltään. Avoimet tietoverkot muodostavat nyt yhteiskunnan viestinnällisen ytimen. Suppeahkon käyttäjäkunnan, harrastajien ja yliopistoväen erillisverkoista on muotoutunut massojen viestintäväline.

Verkkoyhteiskunnan infrastruktuurin yhteydessä on puhuttu tiedon valtateistä, mikä perustuu Yhdysvaltain ja Kanadan 1990-luvun alun informaatioyhteiskuntastrategioihin. Erilaiset fyysisen liikkumisen väylästöt ovat niissä saaneet rinnalleen informaation ja informaatiotuotteiden liikkumista edistävän väylästön eli tiedon valtatien (information superhighways). Tiedon valtatie on terminä havainnollinen. Tunnettu yhdysvaltalainen oikeusinformatiikan tutkija Ethan Katsh onkin sattuvasti kutsunut tiedon valtatietä metaforaksi.

Eurooppalaisittain on varsin yleisesti katsottu, että julkisen vallan on edistettävä infrastruktuureja, niiden kehittämistä, ylläpitoa ja niiden käytettävyyttä. Emme edes voi puhua infrastruktuurista merkittävänä väylästönä, jos se on vain harvojen satunnaisesti käytettävissä tai täysin markkinavoimista riippuvainen. Julkisen vallan tulee siis myötävaikuttaa kulloinkin tärkeiden infrastruktuurien kehittymiseen, vaikka sen ei välttämättä tarvitse itse niitä ylläpitää. Kysymys on yhteisen hyvän ylläpitämisestä.

Yhdysvalloissa on toisaalta esiintynyt ajatuksia, joiden mukaan avointen tietoverkkojen tulisi olla riippumattomia julkisen vallan toimista. Esimerkiksi Christine Borgman on palkitussa, informaation tavoitettavuutta koskevassa teoksessaan ”From Gutenberg to the Global Information Infrastructure” pitänyt tiedon valtatietä harhaanjohtavana metaforana juuri kustannusvastuuta ajatellen. Toteamuksen taustalla on epäilemättä Internetin alkuvaiheiden pyrkimys sääntelystä vapaaseen verkkoviestintään. Viimeistään perusoikeuksiemme käytön siirryttyä merkittävässä määrin verkkoihin tuo ajatus muuttui kuitenkin utopiaksi.

Euroopassa tilanne on jossain määrin toinen. Informaatioinfrastruktuuria ajatellen merkittävä siirtymävaihe aikaisemmasta passiivisesta informaatioyhteiskunnasta uuteen aktiiviseen verkkoyhteiskuntaan tapahtui eurooppalaisittain lähes samanaikaisesti, kun teletoiminta direktiivipohjaisesti avautui Euroopassa 1990-luvulla kilpailulle.

Verkkojen muutos haasteena

Liberalisointia aloitettaessa avoimet tietoverkot eivät televerkoista poiketen vielä olleet varsinainen infrastruktuuri. Nyt ne ovat sitä. Sääntelylle on tullut uusi kohdealue.

Verkkojen muutos hämmensi aluksi niin Euroopan Unionin kuin kansalliset lainsäätäjät. Perinteisten verkkojen rinnalle tuli toisenlainen verkko toisenlaisin toimijoin. Avoin verkko alkoi tulla perinteisten verkkojen

kilpailijaksi. Vähitellen myös puhelut ovat siirtymässä IP-ympäristöön ja osin ohi operaattoreiden Internetiin. Ajan merkkinä sanastokeskus on kesällä 2007 julkaissut kolmikielisen Internetpuhelusanaston.

Viestinnän ja viestintäväylien pitkälle viety sääntely ei ole uusi asia. Esimerkiksi julkisen palvelun radio- ja televisiotoiminnan sääntelyllä on pitkät perinteet. Käsite on peräisin 1800-luvulta Yhdysvalloista silloin teletoimintaan liitettynä. Euroopassa teletoiminnan sääntely on ollut ennen kaikkea teknisistä syistä jo vuosien ajan yksityiskohtaisesti direktiiviohjattua.

Nykyaikainen avoin tietoverkko on sääntelyn kannalta hankala kohde. Lainsäätäjän tulisi ottaa huomioon monia eri asioita alkaen verkon hallinnoinnista ja teknisestä laadusta ja edeten sisältöä koskeviin mahdollisiin rajoituksiin.

Lapsipornografian estoa koskeva laki vuodelta 2007 on siitä hyvä esimerkki. Lailla pyritään operaattoreiden vapaaehtoisuuden kautta rajoittamaan ulkomaisten lapsipornosivustojen käyttöä. Kysymys on siten yhteen vakavan rikollisuuden muotoon vaikuttamisesta. Puhuminen yksipuolisesti sensuurista on tuonut paljon julkisuutta, mutta puhe on myös harhaanjohtavaa. Oikeudellisesti ongelmallisempaa on yksittäisten ihmisten sekä kansalaisjärjestöjen sitominen tiedon tuottajiksi aidon valvontayhteiskunnan hengessä. Erilaiset verkon seuraajat ja käyttäjät raportoivat poliisille. Isoveli valvoo. Kaiken kaikkiaan laki olisi edellyttänyt huolellista tarkastelua perusoikeuksien näkökulmasta. Näin ei kuitenkaan tapahtunut, vaan yksi lainsäädännön laatutekijöistä sivuutettiin.

Teknologinen konvergenssi eli yhdentyminen on tehnyt tiedon valtatien monisisältöiseksi. Siitä ei kuitenkaan välittömästi seuraa kattava ja teknisesti helppo oikeudellinen konvergenssi. Kysymys ei ole vain yhtä tuotetta tai menettelyä koskevasta, vaan uuteen teknologiaan sopeutettavasta sääntelystä. Ja kun verkkoympäristö alkaa nykyisin olla jo kriittistä infrastruktuuria, joudumme pohtimaan myös menettelyjä poikkeustilanteisiin.

Toistaiseksi meiltä puuttuu yhteinen käsitys infrastruktuurista säätämisestä, mutta myös yleislaki informaatioinfrastruktuurista. Tiettyä pohjaa uudelle kokonaisajattelulle saadaan tosin Euroopan unionin vuoden 2002 sähköisen viestinnän kaikkiaan viidestä eri direktiivistä. Emme enää puhu teletoiminasta, vaan sähköisestä viestinnästä.

Direktiivi 2002/21 eli puitedirektiivi on eräänlainen informaatioinfrastruktuurin yleisen sääntelyn direktiivi – direktiivi sähköisten vies-

tintäverkkojen ja palvelujen yhteisestä sääntelyjärjestelmästä. Vaikka direktiivissä on mainittu käyttäjien oikeudet ja kohtuuhintaisuus, se on kuitenkin ensi sijassa kilpailua ja kansallista sääntelyä sen mukaisesti järjestävä ja aikaisemman teletoiminnan liberalisoinnin hengessä annettu direktiivi. Olimme pitkään tottuneet näkemään aikaisemman telelainsäädännön ensi sijassa operaattoreita koskevana sääntelynä.

Samaan direktiiviryppääseen kuuluva sähköisen viestinnän tietosuojadirektiivi sitä vastoin lähtee jo yksilön oikeuksista. Ei tietosuojasta voi enää muusta lähtökohdasta säätääkään. Henkilötietolaki ja sähköisen viestinnän tietosuojalaki kulkevat väistämättä käsi kädessä yksityisyyttämme suojaten.

Kokonaisuutena myös vuonna 2006 komission toimesta käynnistetty sähköisen viestinnän sääntelyn uusimistarpeen arviointi on kuitenkin edelleen ensi sijassa markkinoita arvioiva. Vaikka emme siis enää puhu telelainsäädännöstä, sähköisen viestinnän uudet lainsäädännölliset viitekehykset ja niiden uudistamiskeskustelu ovat valmistelutavastaan johtuen paljossa vanhahtavia. Niissä kuuluu ensi sijassa markkinoiden, ei kansalaisen ääni.

Tiedon valtatie kaipaa liikennesääntöjä

Tiedon valtatie on sikäli kiintoisa metafora, että verrattaessa tiedon ja liikenteen valtateitä havaitaan nopeasti turvattomuuden ero. Liikenteen valtatiellä olemme välittömästi turvalliseksi tarkoitetussa ympäristössä, missä oikeuden merkit ohjaavat turvalliseksi tarkoitettua liikennettä.

Tiedon valtatiellä olemme heti sille liittyessämme riskialttiilla tiellä. Emme tiedä muista kulkijoista tai erilaisista tiellä liikkuvista ja tietoa kokoavista agenteista. Yksityisyyteemme kohdistuu tiedon valtatiellä erilaisia uhkia, mutta myös suoranaisia hyökkäyksiä. Liikennemerkkejä ei näy, mutta siellä täällä on näkyvästi erilaisia – esimerkiksi tekijänoikeuksia koskevia – demokratialle koko lailla vieraita ilmiantopyyntöjä.

Sähköisen asioinnin lisääntyessä käytämme yhä enemmän perusoikeuksiamme tällä turvattomaksi rakentuneella tiellä. Toki moniakin asioita verkkoviestinnässä jo säännellään. Henkilötietolaki koskee myös verkkoa. Sähköisen viestinnän tietosuojalaki täsmentää sitä. Ja yhtä lailla laki sähköisestä asioinnista viranomaistoiminnassa on infrastruktuurilaki.

Sääntely on kuitenkin kehittynyt satunnaisesti ja jäänyt epätasapainoiseksi. Esimerkiksi verkkotunnuksista säädetään laissa, mutta tietoturva

on jätetty toiskätisen sääntelyn varaan niin henkilötietolain kuin sähköisen viestinnän tietosuojalainkin puitteissa. EU:n tietoyhteiskuntaohjelmat sekä oma kansallinen tietoturvastrategiamme puolestaan nojaavat markkinoihin ja parhaisiin käytäntöihin. Kun katsoo, miten parhaita käytäntöjä strategioissa kuvataan, joutuu havaitsemaan niiden epämääräisyyden. Parasta käytäntöä ohjaavat helposti markkinoiden ja byrokratian tehokkuus ja halpuus. Yksilön oikeudet saavat silloin vähemmän huomiota.

Kun ajattelemme tietoverkkojen kasvavaa merkitystä yhteiskunnassa, olisi vakavasti pohdittava niitä periaatteita, joiden varaan avointen tietoverkkojen käyttö tulee rakentaa. Tällöin ainakin tietoturvallisuus, verkkoihin pääsy, halpuus, viestinnän luottamuksellisuus ja oikeus anonyymiin liikkumiseen verkossa ovat arjen tietoyhteiskunnan keskeisiä asioita kansalaisen näkökulmasta. Samaan yhteyteen on liitettävä ajatus oikeudesta tietoon. Tietoverkkojen kautta meidän tulee voida toteuttaa oikeuttamme tietoon hyödyntämällä perustietovarantoja.

Kansalaisen näkökulma näyttää usein käytännössä unohtuvan. Tyypillisen esimerkin tarjoavat ne tilanteet, joissa viranomaisen palvelua televerkossa jonottaneet ovat joutuneet tästä erikseen maksamaan. Vasta eduskunnan oikeusasiamiehen puuttuminen asiaan sai viranomaiset viimein muistamaan kansalaisen oikeudet. Tässä näkyy havainnollisesti hallintovaltion ja oikeusvaltion ajallinen taitekohta.

Oikea tapa edetä parempaan lainsäädäntöön ei voi olla eteneminen haitallisten seuraamusten kautta. Eikä tietoturvallisemman uuden IP-protokollan odottaminen voi olla perustelu sääntelyn hitaalle etenemiselle.

Vastaavasti Euroopan unionin pyrkimys tietoverkkorikosten sääntelyyn jättää materiaalisen oikeuden mentävän aukon sääntelylle. Vanhan teollisen yhteiskunnan tapaan asioita pyritään ratkomaan. Ei säädetä siitä, mikä on olennaista eli asioiden oikeasta järjestyksestä.

Matkalla parempaan lainsäädäntöön verkkoyhteiskunnassa on myös syytä muistaa tietosuoja- ja muiden vastaavien viranomaisten rooli. Kansalaisten tukena tulee olla riippumattomia, ohjaavia viranomaisia, jotka ottavat kantaa siihen, mikä on oikein. Tietosuojavaltuutettu on mitä tyypillisimmin tällainen uuden ajan airut oikeusvaltiossa.

Internet-oikeus vai informaatio-oikeus?

Kun avoimet tietoverkot tulivat yleisempään käyttöön, alkoi samalla uusille ilmiöille tyypillinen oikeudellisten ongelmien tunnistamisen aika. Kuten tavallista syytettiin lainsäätäjää jälkeen jäämisestä. Jos jonkun ilmiön tai tapahtuman nimeä ei löydy lainsäädännöstä, syy pannaan herkästi lainsäätäjän kontolle. Se on myös helpoimpia tapoja herättää huomiota oikeudesta keskusteltaessa. Varsin pian oli myös niitä, jotka alkoivat puhua erityisestä Internet-oikeudesta. Se taas myi hyvin.

Vähemmälle huomiolle jäi se, että avoimet verkot eivät syntyneet neitseellisesti koskemattomaan maaperään. Monet asiat olivat ratkaistavissa ilman lainsäätäjän erityistä aktivoitumista. Esimerkiksi henkilötietolakiin ei meillä sitä vuosina 1995-1997 valmisteltaessa otettu erityisiä verkkosäännöksiä. Laki koski ja koskee kaikenlaista henkilötietojen käsittelyä.

Tänään tilanne on merkittävällä tavalla toinen. Internetin tai oikeammin sanottuna avointen tietoverkkojen muuntuminen yleiseksi infrastruktuuriksi pakottaa pohtimaan sääntelyn yleisiä periaatteita, mutta myös niitä muutoksia, mitkä tiedon valtatie on eri asioihin tuonut.

Esimerkiksi tekijänoikeudesta on todettu, että se on verkkoympäristössä muuttunut ongelmiltaan kopiointioikeudesta (copyright) teoksiin pääsyn oikeudeksi (access). Tämä Jane Ginsburgin toteamus on osuva. Vastaavasti oli Suomessa, ensimmäisenä Euroopassa, tullut tarpeen säätää erikseen laki sähköisestä asioinnista viranomaistoiminnassa. On perusteltua ymmärtää hallinto yhdestä näkökulmasta myös informaatioprosessina.

On selvää, että Internet tarjoaa kiinnostavan ja tärkeän tutkimuskohteen. Jo sen hallinnointi on oikeudellisesti tärkeä asia. ICANN (Internet Corporation for Assigned Names and Numbers), joka hallinnoi verkkoon liittyvien laitteiden ja palvelujen tunnuksia, on poikkeuksellisen tärkeä organisaatio. Sitä on myös tutkimuksen näkökulmasta syytä valvoa, kuten esimerkiksi Michael Froomkin tutkimuksissaan näkyvästi tekee. Maailman tärkeimmän viestintäverkoston hallinnon tulisi olla läpinäkyvää.

Puhuminen Internet-oikeudesta on silti edelleen pikemminkin markkinahakuista kieltä. Cyberoikeus on jo vähemmän esineellinen ilmaisu. Suomalaisittain voitaisiin luontevasti puhua tietoverkko-oikeudesta.

Olennaista on kuitenkin havaita se merkittävä muutos, minkä tietojenkäsittely ja tietoverkot ovat saaneet aikaan informaation ja viestinnän oikeudellisessa arvioinnissa tietoverkkojen yhteiskunnassa. Informaatio

ei enää ole vain raaka-ainetta, vaan keskeinen asia yhteiskunnassa ja tiedon valtatiellä. Toimimme digitaalisessa ympäristössä informaatiota käsitellen.

Informaatio-oikeuden periaatteita

Kun digitaaliseen tietoympäristöön ja siinä toimimiseen yhdistetään ihmisen itsemääräämisoikeutta vahvistava oikeusvaltion kehitys, on ollut tarpeen alkaa aikaisempaa voimallisemmin puhua informaatio-oikeudesta ja sen keskeistä periaatteista. Ei siis EU:n yleisempään tapaan vain informaatiomarkkinoista.

Pohjoismaissa informaatio-oikeuden käsitteen otti ensimmäisenä käyttöön norjalainen Jon Bing jo 1980-luvun alussa. Sittemmin sitä on oikeusinformatiikan puitteissa luonnehdittu oikeudenalaksi, jonka puitteissa tutkitaan informaation tuottamisen, käsittelyn, välittämisen, markkinoinnin, suojaamisen ja säilyttämisen oikeudellista sääntelyä sekä sääntelyn tarvetta ja mahdollisuuksia. Tuomas Pöystin ja Rauno Korhosen väitöskirjat antavat valaisevan kuvan aihepiiristä kansallisesti ja eurooppalaisittain.

Informaatio-oikeuden lähtökohta on selkeä. Kysymys on ihmisen oikeuksista sekä niiden tukemisesta oikeusvaltiossa. Informaatio-oikeus turvaa itsemääräämisoikeutemme toteutumista.

Voimme perustellusti puhua informaatio-oikeuden periaatteista. Niistä keskeisimmät ovat ymmärtääkseni oikeus tietoon, oikeus viestintään, informaation vapaus, informaation kulun vapaus, tiedollinen itsemääräämisoikeus sekä oikeus tietoturvaan.

Periaatteet ovat ihmisoikeusperusteisessa oikeusvaltiossa eräänlaisia metaoikeuksia eli yhteiskuntasopimusten tasoisia tavoitteellisia, moraalisia päämääräoikeuksia. Niistä ei ole perusoikeustasoisia säännöksiä, mutta ne ovat perusoikeuksien selkeitä taustakertomuksia sekä perusoikeuksien toteuttamisen keskeisiä edellytyksiä. Oikeus ei ole vain sitä, mikä on lakiin sellaisenaan kirjoitettu. Jokainen yksittäinen oikeus on kertomus jostain.

(1) Oikeus tietoon

Oikeus tietoon on vallitsevaan ihmiskäsitykseen perustuva keskeinen vapausoikeus. Ihmisellä on aito tarve tietää ja käyttää tietoa. Voidakseen käyttää vapaasti itsemääräämisoikeuttaan oikeusvaltiossa yksilöllä tulee olla oikeus tietoon – sekä itseään koskevaan että yhteiskuntaa koskevaan tietoon.

Kysymys on siten itsemääräämisoikeuden tiedollisesta ulottuvuudesta. Se on meillä lainsäädännössä näkyvimmin ilmaistu kirjastolain hienossa 2.1 §:ssä:

> Yleisten kirjastojen kirjasto- ja tietopalvelujen tavoitteena on edistää väestön yhtäläisiä mahdollisuuksia sivistykseen, kirjallisuuden ja taiteen harrastukseen, jatkuvaan tietojen, taitojen ja kansalaisvalmiuksien kehittämiseen, kansainvälistymiseen sekä elinikäiseen oppimiseen.

(2) Oikeus viestintään

Oikeus viestintään puolestaan on uusi tai ainakin verkkoyhteiskunnassa uudella tavalla esille tuleva metaperusoikeus. Ei ole enää riittävää, että puhutaan erikseen esimerkiksi sananvapaudesta tai luottamuksellisten viestien suojasta tekniikkaneutraaleina vapauksina. Olennaista on myös informaatioinfrastruktuurin yleinen käyttömahdollisuus, kun perusoikeuksia ja niiden suojaa tarvitaan myös tietoverkoissa.

(3) Tiedollinen itsemääräämisoikeus

Tiedollinen itsemääräämisoikeus on itsemääräämisoikeuden yksi peruselementti. Yksilöinä meillä on oikeus olla yksin yhteiskunnassa. Fyysistä yksityisyyttä täydentää verkkoyhteiskunnassa kasvavassa määrin tiedollinen yksityisyys. Digitaalinen identiteettimme kuuluu myös itsemääräämisoikeutemme piiriin.

Itsemääräämisoikeuden puitteissa meillä on lähtökohtaisesti oikeus säilyttää määräysvalta itseämme koskevaan informaatioon, pitää se halutessamme salassa tai julkistaa se yhteiskunnassa. Voimme epäilemättä perustellusti puhua myös eräänlaisesta tiedollisesta kotirauhasta.

Amerikkalainen tapa puhua tiedollisesta omistusoikeudesta on valaiseva. Kun joku käsittelee meitä koskevia tietoja, on aina kysymys ensisijaisesti meidän tiedoistamme. Meitä koskevien tietojen käsittelyn oikeuden tulisi siksi perustua lakiin.

(4) Informaatiovapaus

Informaatiovapauden periaate on demokratian, kulttuurin ja yksityisen talouselämän toimivuuteen liittyvä keskeinen yhteiskuntaperiaate. Informaation tulee muista raaka-aineista poiketen lähtökohtaisesti olla vapaasti käyttävissä yksityisesti, yhteiskunnallisesti, viestinnällisesti ja kaupallisesti. Kansainvälisessä keskustelussa ja monien maiden lainsää-

dännössä informaatiovapaudella tarkoitetaan usein rajoitetummin vain julkisen sektorin tietojen avoimuutta.

(5) Informaation vapaa kulku

Informaation vapaan kulun periaate on yhteydessä ennen kaikkea sivistykseen sekä kulttuuriin. Yhteiskunnan ja yksilöiden tiedollista ja taidollista kehitystä ei saa estää salaisuuksin eikä monopolein. Siksi oikeusjärjestyksessä on varauduttava tiedon vapaan kulun turvaamiseen erityisin oikeuksin ja ennen kaikkea perusoikeuksin.

Tekijänoikeuslainsäädäntö on tässä katsannossa varsin ongelmallista verkkoyhteiskunnan lainsäädäntöä. Jos sitä ohjaa ahneuden henki, informaation vapaa kulku vaikeutuu. Toisaalta, jos vertaisverkkojen avulla tai muilla vastaavilla tavoilla loukataan merkittävästi tekijöiden oikeuksia, tehdyn työn hyvittäminen rajoittuu. Tämän suhteen lainsäädännöllinen järjestäminen kohtaa enenevässä määrin vaikeuksia verkkoyhteiskunnassa.

(6) Tietoturva

Oikeus tietoturvaan on koko uuden verkkoyhteiskunnan informaatio-infrastruktuurin toimivuuden perusedellytys. Demokraattinen yhteiskunta ja oikeusvaltio voidaan rakentaa tietoverkkojen ja informaation varaan vain, jos asianmukaisen tietoturvan avulla voidaan taata infrastruktuurin ja sen käytön toimivuus. Meillä tulee olla oikeus tietoturvaan kuten muuhunkin turvallisuuteen. Tätä ei ole vieläkään asian mukaisesti havaittu kansallisesti tai kansainvälisesti.

Jo nämä informaatio-oikeuden yleiset periaatteet kertovat ymmärtääkseni selkeästi sen, miten tärkeä oikeudenala informaatio-oikeus nykyisin on. Sen vastakohtana on asioiden pirstoutuminen eri oikeudenalojen puitteissa erikseen säänneltäviksi ilman riittävää kokonaiskäsitystä. Tilanteen haittavaikutuksia todistamme päivittäin.

Voidaan kysyä, missä ovat yksityisyys ja julkisuus? Ne ovat näiden metaperiaatteiden lainsäädännöllisiä toteutuksia. Meillä on itsemääräämisoikeutemme puitteissa oikeus niin yksityisyyteen kuin julkisuuteenkin. Ne ovat yksilön oikeuksia, perusoikeuksia.

Jo hakukoneet luovat henkilötietojen käsittelyn ja yksityisyytemme kannalta merkittäviä oikeudellisia ongelmia. Hakukoneet verkkoyhteiskunnan muistina ovat helposti ristiriidassa sen kanssa, että henkilötietojen käsittelyssä on ajalliset rajansa. Euroopan unionin tietosuojatyöryhmä WP29 onkin ottanut hakukoneet vuoden 2008 työskentelyssään erityisen tarkastelun kohteeksi.

Lainsäädännön ja verkon haasteet käyttäjälle

Avointen tietoverkkojen kehitys on oikeudellisessa katsannossa jo kokenut merkittäviä muutoksia. Silloin, kun verkoista ei vielä ollut muodostunut yleistä informaatioinfrastruktuuria, aihepiiri oli oikeudellisesti vain vähän kiinnostava. Monien asioiden uutuus oli näennäistä. Oli vain osattava kysyä oikeudellisesti oikein. Lähinnä Internetin hallinto oli aluksi poliittisesti ja oikeudellisesti kiintoisa aihe.

Tilanne muuttui, kun WWW oli muuttanut verkkojen käyttömahdollisuuksia ja kun niiden laajamuotoinen kaupallinen käyttö alkoi. Aluksi vain harva asia vaati erityissääntelyä. Esimerkiksi henkilötietolakiin ei, kuten edellä on todettu, vielä otettu erityisiä tietoverkkosäännöksiä. Yleisiä säännöksiä voitiin soveltaa myös verkkotilanteisin.

Nykyisin tietoverkot infrastruktuurina puolestaan jo edellyttävät oikeusvaltiossa kehittynyttä oikeudellista sääntelyä. Kun kansalaisen on demokratian erään keskeisen ajatusmallin mukaan tunnettava laki ja noudatettava sitä, merkittävä infrastruktuuri ei saada jäädä sääntelemättä, eikä myöskään vain ammattilaisten hallitseman sääntelyn varaan. Samalla on tultu kauas siitä avointen tietoverkkojen alkuperäisajatuksesta, jossa tavoitteena on ollut toimia paljossa oikeudellisesti sääntelemättömässä tilassa.

Lainvalmistelussa on olennaista paitsi teknologian kehityksen ja ihmisen oikeuksien suhteen tarkkailu, myös soveliaan lainsäädäntötekniikan löytäminen. Meillä on onnistuttu etenkin tietotekniikkaan liittyen vakiinnuttamaan käyttöön teknologianeutraalin lainsäädännön ajatus. Lainsäätäjä sääntelee ensisijaisesti tekoja, ei niinkään teknologiaa sinänsä. Näin lainsäädäntö lepää kestävämmällä pohjalla teknologian muuttuessa.

Lainsäädännön informatiivisuus voi kuitenkin kansalaisen kannalta jäädä puutteelliseksi. Lainsäädännössä ei esimerkiksi toistaiseksi puhuta tietoteknisistä viruksista, mutta niiden tekeminen, levittäminen ja ohjeistaminen ovat rangaistavia vaaran aiheuttamisena tietojenkäsittelylle. Ja sana haittaohjelma mainitaan vain sähköisen viestinnän tietosuojalaissa.

Yksi paremman sääntelyn tavoitteista pitäisikin olla käyttäjän ymmärrettävämpi oikeudellinen ohjeistaminen. Selventämistä tarvitaan, vaikka jo eettisten tuntojemme pitäisi estää ainakin suuri osa luvatonta toimintaa verkoissa.

Julkisella sektorilla julkisuuslain 18 § on toki ollut askel lisääntyvän oikeudellisen tietoisuuden suuntaan. Tuo hyvän tiedonhallintavan sisäl-

tävä säännös velvoittaa kouluttamaan käyttäjät työnsä oikeudelliseen viitekehykseen. Koulutusta vain on ainakin toistaiseksi ollut luvattoman vähän. Hyvä ajatus ei ole toteutunut. Julkisuusperiaatteen merkitystä korostavana säännös saattaa myös johtaa yksityisen sekä julkisen suhteen vääristymiseen julkisessa toiminnassa.

Matkalla arjen tietoyhteiskuntaan on epäilemättä monta vaaraa edessä. Yleisemmin kysymys on yhteiskunnasta sinänsä. Lainsäädännön osalta kysymys on perusoikeuksiemme, ennen kaikkea yksityisyyden, vaarantamisesta. Käyttäjien kohdalla on lisäksi syytä kiinnittää huomio siihen, miltä tietoverkko käyttäjän silmissä näyttää.

Arjen tietoyhteiskunnan jännitteet

Arjen tietoyhteiskunta on epäilemättä myönteinen ja myönteiseksi tarkoitettu käsite. Hyödynnämme arkipäivässä tietotekniikan saavutuksia. Ongelma on vain siinä, että niin kansallisesti kuin kansainvälisesti, myös hallinto etsii tehokkaita tietotekniikan sovellutuksia. Olemme matkalla sekä arjen tietoyhteiskuntaan että valvontayhteiskuntaan.

Yleisen ja erityisen välisessä suhteessa erityinen usein, ehkä useimmiten sivuuttaa yleisen. Erikoistuminen syventää ja samalla kertaa kaventaa osaamista. Kun kaikki hallinnon sektorit omalta osaltaan optimoivat tietotekniikan tuoman tehokkuuden, on Vance Packardin vanha 1960-luvun ajatus alastomasta yhteiskunnasta hyvin lähellä. Alaston tosin on ensi sijassa kansalainen.

Lainsäädännön tasolla kysymys on paljossa perusoikeuksien, erityisesti yksityisyyden tunnistamisesta lainvalmistelussa. Yksityisyys suhdekäsitteenä on pirstaleisessa lainsäädäntötyössä vaikea asia. Meillä kaikilla, pääministerilläkin, on kiistatta oikeus yksityisyyteen. Ilman tuota lähtökohtaa olisi turha puhua demokraattisesta oikeusvaltiosta. Eikä yksityisyyttämme ole lupa jättää markkinavoimien haltuun, vaikka sananvapauden varjolla niin pyritään toisinaan tekemään.

Olisi houkuttelevaa, mutta lyhytnäköistä määritellä yksityisyys kattavasti kaikkea hallintoa, kaikkea lainvalmistelua ja kaikkia markkinoita silmällä pitäen. Yhteiskunnan ja tietotekniikan nopeassa muutoksessa se olisi pian kadotettua yksityisyyttä. Käsite ei vastaisi yhteiskunnallista todellisuutta ja sitä jouduttaisiin alinomaa muutamaan.

Oikeampaa olisi luoda kestäviä yleisiä oppeja yksityisyydestä myös lainvalmistelijoiden käyttöön, vaikka aina sekään ei riitä. Esimerkiksi tekeillä oleva Lex Nokia eli työnantajan tarkkailun lisääminen työpaikoilla yhteisötilaajien sisäisessä viestinnässä on tästä hyvänä esimerkkinä.

Yksityisyyttä työpaikalla halutaan supistaa juuri, kun se on maallemme mainetta tuoden saatu säädettyä. Samanaikaisesti kun Saksassa perustuslakituomioistuin helmikuussa 2008 torjuu ajatuksen kansalaisten tietokoneiden ja viestinnän tiukasta valvonnasta (online-durchsuchung), meillä lainvalmistelijat markkinoiden toivomuksesta luottavat jääräpäisesti talouden voimaan.

Julkisella sektorilla ongelmana on yhtä lailla se, millä tavoin lainsäädäntöä viranomaista sivuilla kuvataan. Ei ole harvinaista nähdä lakilistaa, mikä alkaa julkisuuslaista ja etenee henkilötietolakiin. Silloin kun kysymys on yksityisyydestämme, etenemisjärjestys on väärä. Lähtökohtana on aina henkilötietolaki. Julkisuuslaki tekee siitä vain vähäisiä poikkeuksia.

Viestinnän konvergenssin myötä myös media on näkyvästi siirtynyt verkkoihin. Samalla osa median vallankäytöstä ilmenee verkoissa. Sen sekä eräiden verkkoyhteisöjen toimesta oikeudellisesti merkittävät käsitteet ovat osin saamassa outoja vivahteita. Niinpä sananvapaus näyttää kelpaavan selitykseksi mitä erilaisimpiin ihmisen oikeuden viestinnällisiin loukkauksiin. Tieto siitä, että yksityisyyden merkitys oikeusvaltiossa on lakisääteisesti kasvanut jää mediassa usein näkymättömiin.

Verkkoyhteiskunnassa ei tietenkään ole kysymys vain median toiminnassa verkoissa. Kiinnostavaa on myös se, miten julkinen valta viestii. Tässä suhteessa on ollut näkyvillä selvä liike neutraalista viestinnästä markkinointiin. Kenties erikoisinta on, että loppuvuodesta 2007 lukuisat julkisen sektorin sivustot varustettiin valtiota työnantajana mainostavin linkein. Tällaisia pyrittiin saamaan jopa riippumattomien tuomioistuinten sivuille.

Kolmas arjen tietoyhteiskunnan keskeinen vaaratilanne syntyy käyttöliittymien ja selainten tasolla. Tiedonhaku ja kopiointi ovat arkisen toiminnan työtapoja. Ne on helppo toteuttaa. Valtavat tietomäärät ovat muutaman näppäimen päässä. Tähän on tultu eikä tästä taida olla paluuta. Silloin oikeudellisen yleissivistyksen merkitys kasvaa sen osoittajana, mikä kulloinkin on oikein.

Havainnollisen esimerkin tarjoaa kysymys työnhakijan tai työntekijän tietojen etsimisestä tietoverkoista. Se on yksiselitteisesti kiellettyä ilman asianomaisen suostumusta. Laki yksityisyyden suojasta työelämässä on tässä suhteessa erinomaisen selkeä. Tietosuojavaltuutetun lain mukaisen kannanoton meillä syksyllä 2006 kohtaama kritiikki juonsikin paljossa juurensa verkkokeskustelijoiden oikeudellisesta sivistymättömyydestä.

Lopuksi

Arjen tietoyhteiskunnassa yksilöä koskevan tiedon tie rekisteröivästä sensorista tai matkaviestimen koodista aina informaation tuhoamiseen tai arkistointiin on entistä pidempi ja monimuotoisempi. Yhä useammin siihen liittyy tavalla tai toisella pistäytyminen tiedon valtatiellä. Tällä pitkällä matkalla on syytä muistaa oikeuden valtatien merkitys.

Sääntöjen matka ihmisoikeuksista yksittäiseen tulkintatilanteeseen on pitkä ja vaikea. Sitä ohjaa kaikissa tilanteissa ihmisen oikeuksien kunnioittaminen. Tätä ei aina muisteta. Niinpä esimerkiksi henkilötunnusta pyritään yhä edelleen käyttämään voittopuolisesti ihmisten tunnistamiseen, vaikka se tarkoitettu yksilöintiin. Varsinaisessa tunnistamisprosessissa henkilötunnus on – jos sitä ylipäätään tarvitaan, vain yksi osatekijä. Kun jopa näin alkeellista erhettä on ollut liki mahdotonta kitkeä pois useassa vuosikymmenessä, arjen tietoyhteiskunnan taivaalla on epäilemättä jo valmiiksi koko joukko oikeudellisen osaamattomuuden mustia pilviä.

Arjen tietoyhteiskunnassa ei ole yksityisyyttä

Risto Heinonen

Nyky-yhteiskunnassa ihmisten toimintoja ja tapahtumia rekisteröidään ja niitä koskevia tietoja käytetään tavoilla, joita ei voitu kuvitellakaan ennen tietokoneita ja tietoverkkoja. Kun kansalainen käy kaupassa, pankissa tai asioi virastossa, kun hän käy kirjastossa tai lääkärissä, jokainen käynti rekisteröidään. Hänen käyttäytymisensä kirjataan yksityiskohtaisesti ja hänen oikeuksiaan ja edellytyksiään arvioidaan näiden tietojen perusteella.

Julkinen valta pitää tuhansia rekistereitä, joista melkoinen osa käsittää koko väestön. Sektoriviranomaisilla on lukemattomia rekistereitä. Kunnat kirjaavat asukkaansa lukuisiin rekistereihin. Yksityiset organisaatiot pitävät omia, usein laajojakin rekistereitä.

Keskiverto suomalainen on hyvinkin 150 rekisterinpitäjän tietojärjestelmissä. Rekisteriin kirjataan ihmisestä kymmeniä, ehkä satoja tietoja. Tietokoneissa käsitellään taukoamatta kymmeniä miljardeja suomalaisten yksittäisiä tietoja.

Arjen askareet perustuvat yhä enemmän tietoverkkojen käyttöön. Kun käytetään verkkojen kautta palveluja ja toimintoja, niiden käytöstä jää aina tieto tapahtumasta. Tapahtumatieto on sähköinen jälki. Tietoja tuottavat tietokoneen tai muun verkon kautta käytettävän laitteen näppäimen tai hiiren painallukset tai kortin tai koodin luenta lukulaitteella. Tietoja tapahtumista kerätään kaikkialla, missä tietojenkäsittelyllä on kyky rekisteröidä ja säilyttää tietoja.

Ubiikkiympäristön tiedonkeruu

Tietoyhteiskunta kokoaa kansalaisen jalanjäljet

Surfailu ja asiointi tietoverkoissa jättävät paljon jälkiä. Surfailusta jää jälkiä oman tietokoneen ohella ainakin organisaation sisäisten verkkojen palvelimiin, tietoliikennettä ja verkon toimintoja ylläpitäviin palvelimiin sekä verkossa palveluja tarjoavien ja sivustoja esittävien osapuolten palvelimiin. Tietoja kerätään kävijöistä, heidän hakemistaan tiedostoista ja sivuista, käytetyistä palveluista, liikkumisesta sivuilla ja tietojen siirroista tai latauksista.

Kuuliaisina ihmisinä kannamme mukanamme erilaisia kortteja - luottokortteja, asiakaskortteja, matka- ja kulkukortteja ja lukuisia muitakin kortteja. Kortin käyttö yleensä yhdistää tapahtumatiedot haltijansa tietoihin. Korttien ja muidenkin älykkäiden laitteiden käyttö kirjaa toimintaamme ja kertoo tavoistamme ja mieltymyksistämme. Käyttötiedot voivat paljastaa jopa ajatteluamme. Korttien ja vastaavien laitteiden käyttöjen pohjalta pystytään rakentamaan meitä kuvaavia profiileja.

Tapahtumatiedoissa merkittävää on se, että niitä kertyy valtava määrä. Yksittäisestä ihmisestä kerätään vuosittain ehkä kymmeniä tuhansia tapahtumatietoja. Tapahtumatietoja ei lainkaan kerätä perinteisessä rekisterinpidossa – paperimuotoisesta asioiden käsittelystä puhumattakaan. Ongelmaksi onkin alettu kokea se, että tietovarastoissa on liikaa tietoja. Samalla kuitenkin uudet tiedon louhinnan, käsittelyn ja analysoinnin välineet helpottavat tiedonhakua ja hyödyntämistä erilaisiin tarkoituksiin.

Kaikki kehitykseen vaikuttavat tekijät viittaavat siihen, että tapahtumatietojen keruu ja erityisesti käyttö lisääntyvät jatkuvasti. Eletään murrosvaihetta, jossa perinteisestä rekisterinpidosta siirrytään verkottuneeseen tietojenkäsittelyyn ja sähköiseen asiointiin.

Siirtymä kasvattaa edelleen tapahtumatiedon määrää. Kun esimerkiksi siirrymme kortilla ja verkossa tapahtuvaan asiointiin, kasvaa tunnistettavien jälkien määrä osto- ja maksutapahtumasta helposti monikymmenkertaiseksi käteismaksuun verrattuna. Tällaisten tapahtumista kertyvien tietojen määrä on jo paljon suurempi kuin kyselyjen perusteella rekistereihin kirjattavien tietojen määrä.

Ubitekniikka kerää tietoa kaikkialta

Kaikkialla läsnä olevaa tietotekniikkaa kutsutaan ubiikiksi tai ubitekniikaksi. Ubitekniikka on tunkeutumassa ihmisen elämisen kaikille alueille. Sen avulla tunnistetaan käyttäjä ja kootaan tietoa hänen toimista huomaamattomalla tavalla erilaisia palveluja tai seurantaa varten.

Ubitekniikka sulautuu alueille, missä sitä ei aiemmin ole käytetty, kuten tilojen rakenteisiin, vaatteisiin tai kodinkoneisiin. Koska tekniikan käyttöalueet laajenevat, laajenevat myös mahdollisuudet havaintojen tekoon ja niiden rekisteröintiin. Samalla käytettäväksi tulee aiempaa valtavasti enemmän ihmisten hyvinkin yksityistä tietoa.

Ihmisillä on tänä päivänä ja ubiikkitekniikan ympäristössä vielä paljon varmemmin mukanaan erilaisia välineitä, joita voidaan seurata, tunnistaa ja paikantaa. Niiden avulla on mahdollista rekisteröidä ihmisten tekemisten ja liikkumisten ohella heidän emotionaalisia tuntemuksiaan-

kin, kuten stressiä, pelkoa tai kiihtymystä. Laitteet voivat rekisteröidä terveydentilaa ja lähettää siitä tarvittaessa tietoja eri tahoille. Tällaisia laitteita on tulossa ympäristöömme ja vaatteisiimme – niitä voidaan jopa upottaa meihin.

Jokainen tällainen tietoa keräävä, tunnistava tai paikantava laite, jota käytämme tai jonka havainnointialueella liikumme, voi rekisteröidä sen käyttöä tai liikkumista. Myös kuva ja ääni on mahdollista tallentaa.

Kaikkialla olevan tietojenkäsittelykyvyn avulla voidaan ihmisistä kerätä massiivisia määriä tietoja, joita ei aiemmin ole ollut mahdollista saada käyttöön. Kun tietojen käsittely- ja säilytyskustannukset ovat alentuneet, tietoja voidaan säilyttää lähes pysyvästi ja hakea tarvittaessa käytettäväksi. Ubiympäristö kiihdyttää tietojen keruun ja ennen kaikkea käytön prosesseja.

Ubitekniikka tarjoaa monia selkeitä hyötyjä, kuten parempia palveluja, vaivattomampaa asiointia ja lisää turvallisuutta. Se lisää ihmisten mahdollisuuksia kertoa itsestään ja tarpeistaan muille. Näihin hyötyihin, myös ns. älykkään kodin mukavuuksiin, liittyy kuitenkin kääntöpuoli – alati paisuva ja jatkuvasti täydentyvä tietojen ja sähköisten jälkien virta. Tämän tietovirran väärinkäyttö tai käyttö ihmisten elämää haitallisesti valvoviin tarkoituksiin on yhtä mahdollinen tulevaisuuden visio, kuin helpottuvat palvelut.

Elämisellä ubimaailmassa on se huolestuttava seuraus, että tapahtumien rekisteröinnin yhteydessä jätetään täysin tahattomasti jälkiä, joista ei välttämättä olla tietoisia. Lisäksi kehittyneet tietojen hakuvälineet keräävät tietoja sellaisistakin paikoista, missä niitä ei tiedetä tai kuvitella olevan. Älykkäässä ympäristössä voidaan käyttää ja yhdistellä erityyppisiä tietoja erilaisista lähteistä.

Erilaisista jäljistä voidaan myös rakentaa yksityiskohtaisia kuvauksia tai profiileja ihmisistä. Nämä profiilit saattavat elää verkossa omaa elämäänsä, josta asianomainen itse ei välttämättä tiedä mitään. Käytännössä mikä tahansa verkkoon koottu tieto voi kääntyä ihmisen hyödyksi tai haitaksi – riippuen siitä, kuka sitä tulee myöhemmin käyttämään ja millaisten tietojen yhteydessä.

Jalanjäljistä rakentuu profiili

Uusimmat teknologiat ovat aiempaa tehokkaampia ja pienikokoisempia, mutta ne mahdollistavat myös mitä erilaisimpien tietojen keruun, käsittelyn ja käytön. Ne ovat muuttaneet valvonnan luonnetta. Valvonta on enenevästi ihmisten ja tapahtumien etäseurantaa tunnistavien ja pai-

kantavien välineiden avulla. Ubiikkiyhteiskunnassa jälkiä jää jatkuvana virtana.

Uusia valvontajärjestelmiä voi arvioida kohteidensa jäljitettävyyden perusteella. Yhä useampi ihminen kantaa mukanaan sähköisen yhteydenpidon ja seurannan välineitä. Esimerkiksi matkapuhelimet on mahdollista paikantaa, niiden yhteyksiä voidaan jäljittää ja liikkumista seurata. Mitä enemmän osapuolet ovat sähköisesti yhteydessä keskenään, sitä enemmän kontakteista kertyy jäljitettävää tietoa. Henkilön kontaktiverkostosta voidaan myös helposti rakentaa kuvauksia.

Teknologiat ovat vaikuttavimmillaan, kun niistä tulee kaikkialla olevia, ubiikkeja. Tällaisia teknologioita on kehitetty lukemattomiin arkipäivän tilanteisiin. Ubiteknologian avulla ihmisten käyttäytymistä kyetään rekisteröimään ja seuraamaan hyvin yksityiskohtaisesti ja kattavasti. Näkymättömien teknologioiden avulla kaivellaan tietoja lähes mistä tahansa lähteistä ja paikoista.

Ubiyhteiskunnassa on tarjolla työkaluja suurtenkin tietomäärien käsittelyyn ja analysointiin. Näiden myötä kaikenlaisista tapahtumatiedoista on tulossa arvokkaita paitsi palvelujen, myös valvonnan kannalta. Niiden avulla etsitään tietomassoista ennalta tuntemattomiakin syy-seuraus-suhteita päätöksenteon avuksi. Työkaluja on käytetty yksityisellä sektorilla erityisesti asiakastietojen analysoimiseen.

Weberiläiselle hallinnolle riitti tilastollinen tieto kansalaisten kontrolloimiseksi. Ubiikki yhteiskunta on kiinnostunut yksilön sisäisestä elämästä, hänen ajatuksistaan ja motiiveistaan. Erilaisiin lokeihin kerättyjä tietoja käytetään arvioimaan sitä, miten ihmiset toimivat eri rooleissaan, kansalaisina, työntekijöinä, asiakkaina ja kuluttajina.

Ihmisten tietovalvontaan käytetään enenevästi profilointia. Aiemmin piirrettiin ihmisistä profiileja yhdistelemällä tietoja eri rekistereistä. Nyt profilointi käyttää hyväkseen myös ubiikin tietojenkäsittely-ympäristön tuottamia tapahtumatietoja. Pankit, vakuutuslaitokset ja kauppa profiloivat asiakkaitaan kaikenlaisten tapahtumatietojen perusteella. Myös viranomaiset ovat löytäneet menetelmän. Turvallisuusviranomaiset etsivät rikollisiksi epäiltyjä, jokainen lentomatkustaja on väritetty riskiprofiilinsa mukaisesti. Kunnat houkuttelevat asukkaikseen hyviksi veronmaksajiksi profiloituja.

Mitä enemmän ihminen tukeutuu verkkoon tekemisissään, sitä todennäköisemmin ja laajemmin tulevat tiedot hänen intresseistään ja asenteistaan ja käytöksestään osaksi hänestä rakennettua profiilia. Mitä innokkaammin surfailija liikkuu sivulta toiselle, sitä yksityiskohtaisem-

man profiilin palveluja verkossa tarjoava hänestä piirtää. Kun ihminen liikkuu ubiympäristössä kännykkää näpytellen ja tunnistimia vilautellen, hän ei tiedä piirtävänsä samalla profiiliaan eri tahoille.

Hämärtyvät rajat ja tietojen yhdistely

Ubiikkiyhteiskunnan päivittäisissä rutiineissa tullaan ylittämään kaikki mahdolliset yksityisyyden rajat. Ubiikissa tiedonkäsittelyssä katoavat helposti ja yksilön huomaamatta fyysiset rajat, seinät, ovet ja vaatteet sekä loogiset rajat, kuten suljetut ja suojatut viestit ja muut yhteydet.

Samoin ylittyvät sosiaaliset rajat. Odotukset luottamuksellisuudesta perheissä, työpaikoilla, pankissa ja kaupassa. Tilaan sidotut yksityisten ja julkisten, avoimien ja suljettujen alueiden välillä olevat rajat hämärtyvät. Valvonta tunkeutuu yksityisyyden perimmäiseen ytimeen – iholle, ihon alle ja pään sisällekin. Panoptisen valvonnan periaatteiden mukaisesti rajoja ei välttämättä ylitetä, mutta luodaan tilaisuuksia ylityksille ja annetaan ymmärtää, että ne voidaan koska tahansa ylittää.

Ihmiset osallistuvat näihin yksityisyyden rajojen ylityksiin pitämällä mukanaan ja käyttämällä kortteja, puhelimia ja yleensäkin kaikenlaisia tunnistettavia, paikannettavia ja jäljitettäviä laitteita. Ne lupaavat apua päivittäisiin tekemisiimme, mutta ne eivät koskaan muistuta seurauksistaan yksityisyydelle. Näistä ihmisaistien älykkäistä jatkeista on tulossa sähköisiä kahleita, joiden avulla käyttäjän toimia ja liikkeitä seurataan.

Tiedonhakuteknologiat ovat yksi ubiikin tietojenkäsittelyn peruskivistä. Tapahtumien rekisteröinnit ja tietojen säilytykset erilaisissa varastoissa eivät ole käyttökelpoisia, ellei ole tehokkaita välineitä suurten tietomäärien hakuuan käsittelyyn ja yhdistelyyn. Kyky yhdistellä eri lähteistä harmittomiakin tietoja, kuten liikkumista, yhteydenpitoa, pukeutumista tai syömistä koskevia tietoja, joita ubiikki ympäristö tuottaa, muodostaa uuden haasteen yksityisyydelle.

Ihmisiä arvioidaan ja luokitellaan yhä useammin heistä eri paikkoihin tallennettujen tietojen perusteella. Kokoamalla tietoja eri lähteistä ja rakentamalla näistä yksityiskohtaisia kuvauksia ja profiileja kavennetaan aina radikaalisti yksityisyyden alaa.

Profiilit on rakennettu vastaamaan ennen kaikkea rakentajiensa tarpeita, ei niiden, joita ne esittävät. Kohde kutistetaan, venytetään tai karsitaan sopimaan näihin tarpeisiin. Profilointeihin löytyy vaivattomasti oikeutus, kuten kaupan, pankkien, vakuutuslaitosten ja yhä useammin myös julkisen hallinnon käytännöt osoittavat.

On esitetty pelkoja, että henkilöprofiileja rakennetaan ennustamaan eitoivottavia tapahtumia ennen kuin ne toteutuvat tai löytämään jo toteutuneiden tekijöitä. Ihmiset, joiden profiilit täyttävät asetetut kriteerit, tullaan asettamaan yhä tarkemman valvonnan kohteiksi. Lentomatkustajat, joiden riskiprofiili värjäytyy keltaiseksi, ohjataan tarkempaan tutkintaan, punaisen profiilin omaavat otetaan heti lähtöportilla talteen. Yhdysvalloissa useiden osavaltioiden koulut profiloivat oppilaitaan mahdollisina väkivallantekijöinä. Suomessa saa varoa profiloitumasta rikoksesta epäillyksi.

Tietokoneistus 1970-luvulla aiheutti suurta huolta yksityisyyden säilymisestä. Yksityisyyden maisema ubiikkiyhteiskunnassa poikkeaa keskitetyn tietojenkäsittelyn maisemasta paljon huolestuttavammalla tavalla. Tietojenkäsittelyn saumaton integroituminen koko elämään tunkeutuu syvästi yksityisyyteen. Valvontakapasiteetit kasvavat paljon yli perinteisen tietojenkäsittelyn. Ubiteknologian kehitys tuottaa välineet yksityisyyteen tunkeutumiselle tavalla, jolla ei ole vertaa ihmiskunnan kirjoitetun historian aikana.

Yksityisyyden ja ubiikin tietojenkäsittelyn leikkauspisteessä toteutuu panoptinen painajaisuni: ympäristömme sisältää näkymättömiä tunnistimia ja lukijoita, jotka seuraavat ympäristöään ja viestivät keskenään havainnoistaan, joita voidaan säilyttää pysyvästi ja palauttaa käyttöön tarvittaessa. Emme ehkä huomaa seurantaa tai edes tiedä siitä mitään, mutta meidän on viisasta olla valppaina sen suhteen. Ellei sosiaalisilla, laillisilla tai teknisillä käytännöillä pyritä rajoituksiin, ei ehkä tule olemaan mitään toimintaa tai paikkaa, missä tavalliset ihmiset kykenisivät välttämään valvontaa. Kotimme ja kehommekin voivat olla herkkien tuntosarvien tunnusteltavina.

Ubiikki tietojenkäsittely käynnistää lukuisia yksityisyyden kannalta ongelmallisia prosesseja, jotka lisäävät yksilöä koskevien tietojen rekisteröintiä, kykyä hakea ja käyttää häntä koskevia tietoja ja seurata häntä. Varmaa on, että lähes jokainen ubiyhteiskunnan aikaansaannos - turvallisemmat kadut, halvemmat yhteydet, paremmat julkiset palvelut, mukavampi ostoksilla käynti, laajemmat valikoimat tai räätälöidyt palvelut - edellyttää henkilötietoja ja ottaa palan pois yksityisyydestä.

Kontrollin katoaminen tiedonhallinnasta

Uusiin teknologioihin liittyvät yksityisyyden arviot lähtevät siitä, että yksilö menettää niiden myötä tietojensa hallinnan. Heti, kun yksilöä koskevia tietoja on viety järjestelmiin tai luovutettu verkon yhteisöpalvelujen sivustoille, hänen mahdollisuutensa hallita niitä heikkenee oleellisesti. Hänen on lähes mahdoton enää poistaa niitä verkosta. Tätä

pidetään eräänä suurimmista yksityisyyden uhkatekijöistä.

> ”Kontrollin menetys omiin tietoihin merkitsee tiedollisen itsemääräämisoikeuden menetystä. Mahdollisuus kontrolloida tietojaan on ehdoton edellytys sille, että yksilö kontrolloi elämäänsä”
>
> *(Wright, 1995)*

Yksityisyyden hallinnan riittämättömyys on käynyt selväksi erityisesti sähköisen osallistumisen ja asioinnin edetessä. Siirtymä paperipohjaisesta ja fyysisestä asioinnista sähköiseen muuttaa asioinnin kontrolloitavuuden yksityisyyden kannalta perusteellisesti. Osallistuminen yhteiskuntaan korttien, matkapuhelinten tai verkkoyhteyksien avulla voi lisätä yksilöiden kykyä seurata asiansa käsittelyä. Se vähentää varmuudella heidän kykyään kontrolloida yksityisyyttään.

Keskitetyssä tietojenkäsittely-ympäristössä on helppo paikantaa tietoja keräävä ja käyttävä taho. Hajautetussa verkkoympäristössä tiedetään periaatteessa tapahtumia kirjaavat tahot, toiminnot ja laitteet. On kuitenkin työlästä osoittaa paikkaa tai tapahtumaa, missä tietoja kulloinkin kerätään, käytetään ja säilytetään.

Ubiikissa ympäristössä tietoja käsitteleviä laitteita on kaikkialla ja tietojen käsittely on häivytetty katseilta ja samalla tietoisuudesta. Kun tietojen käsittely sulautuu ympäristöönsä, ihmisellä on toivoton tehtävä arvuutella, mihin korttien, puhelinten ja muiden tunnistimien käyttöjen ja liikkumisten tunnistin on piiloutunut. Lisäksi hänen on lähes mahdoton arvioida tietojensa käsittelyn asianmukaisuutta.

Rekisteröityjen oikeutta arvioida tietojensa käsittelyä ja vaikuttaa siihen on ubiympäristössä hankala toteuttaa, eivät osaa vaatia oikeuksiaan tai jos osaisivat, eivät tietäisi, kenelle vaatimuksensa kohdistaisivat. Tällaisessa ympäristössä on työlästä etsiä tietojen käsittelystä vastuullisia tahoja. Siellä on ylipäätään vaikea tietää, miten ja milloin yksityisyyteen on puututtu. Epäselvää voi olla sekin, mitä yksityisyys ja sen loukkaaminen käsitteenä voisivat ubiikissa maailmassa olla.

Uusi tapa asioida ja kontrolloida asiointia ei aiemmasta poiketen ole sidoksissa paikkaan tai etäisyyksiin. Se ei tunnusta fyysisiä, hallinnollisia tai poliittisia rajoja. Se ei ole riippuvainen ajasta. Se tapahtuu tässä ja nyt, mutta takaa tietojen pysyvyyden ja niiden myöhemmän käytön koska tahansa ja missä tahansa.

Kulloisestakin kontrollista ollaan yhä vähemmän tietoisia ja asioiva osapuoli osallistuu valvontaansa tietämättään. Valvojakaan ei välttämättä tiedä käyttämiensä tietojen lähteitä, ehkä tiedot on kerätty aivan muihin tarkoituksiin.

Piiloutuva tiedonkeruu

Ubiympäristössä tietojen käsittelyn prosessi hallitaan huonosti. Yksityisyyden kannalta ongelmana on erityisesti tietojen keruun ja käytön erillisyys. Aina eivät edes tietojen käsittelijät tiedä, missä vaiheessa tietoja kertyy, miten niitä säilytetään tai kuka niitä käyttää ja mihin tarkoituksiin.

Kun tietoja kertyy automaattisesti, ei välttämättä ole suunniteltu, mihin kaikkeen niitä käytetään. Jälkikäteen löydetään uusia käyttöjä, jos esimerkiksi tietoja analysoitaessa löytyy ennalta arvaamattomia, mutta merkittäviä syy-seuraus-yhteyksiä.

Tietoja kerätään, kun ollaan yhteydessä palveluihin, tapahtumiin ja toimintoihin tai ylipäätään liikutaan tällaisten vaikutusalueilla. Hyvin huomaamattomat ja vähäiset toimet, huolimaton näppäimen painaltelu tai hiiren klikkailu tai korttien ajattelematon vilauttelu saatetaan ubiympäristössä tulkita suostumukseksi tietojen käsittelyyn.

Ubiympäristössä tietoja kerätään ja käsitellään yleensä ilman ihmisen aktiivista toimintaa. Kun ihminen ”osallistuu” toimintoihin, hän ei välttämättä tiedä, missä palveluissa ja toiminnoissa hän on käynyt, kuka niitä pitää, mitä merkintöjä käynneistä jää tai mihin niitä käytetään. Aidon suostumuksen antaminen tällaisiin käsittelyihin voi olla mahdotonta. Ei välttämättä edes tiedetä, mihin tai kenelle suostumus annetaan, ei myöskään voida selvittää, mitä siitä seuraa yksityisyydelle.

Ihmiset, joiden tietoja haetaan rekistereistä tai kaivellaan ubiympäristön kaikenkirjavista lähteistä, eivät voi vaikuttaa tähän yksityisyyteensä puuttumiseen juuri muuten kuin jättäytymällä ulkopuoliseksi. Heidän pitää luopua matkapuhelimesta, kaikista korteista ja lopettaa tietoverkon käyttö. Tärkeä paikka, mihin ihmiset ovat vetäytyneet nauttimaan yksityisyydestä, on ollut auto. Tämä yksityisyyden yksi viimeisistä saarekkeista tulee sekin tarkan valvonnan piiriin, kun suunnitelmat autoilun sähköisestä seurannasta toteutuvat.

Julkisen sektorin toteuttamilta rekisteröinneiltä ja valvonnalta on hankala välttyä, siellä tietojen keruu ja käyttö sekä kansalaisten kontrolli ovat yleensä lakien mahdollistamia ja velvoittamiakin.

Yksityisellä sektorilla sähköisten jälkien jättämistä on ainakin periaatteessa mahdollista välttää, jos ihminen vain tietää, milloin jälkiä jää. Ongelmana siellä on, että jälkiä jää hyvin huomaamattomasti, jälkien jättämistä ja niiden käyttöä on vaikea kontrolloida. Tosin erottelu julkiseen ja yksityiseen sektoriin on tässä keinotekoinen, koska kummallakin on yhä yleisemmin pääsy toistensa tietoihin.

Ennakoimattomat tiedon käyttötavat

Ihmisiä, heidän edellytyksiään, kelpoisuuttaan, ominaisuuksiaan ja persoonallisuuttaan arvioidaan yhä useammin heidän tietoverkoissa käyttäytymisensä sekä verkkoihin jättämiensä tietojen ja jälkien perusteella. Tällaiset arviot voivat levitä laajalle verkkoon. Niitä on mahdollista käyttää monenlaisiin tarkoituksiin ilman, että asianomainen tietää siitä mitään ja voi vaikuttaa siihen mitenkään.

Sähköiset minämme kiertelevät verkoissa kontrollimme ulottumattomissa, edustavat meitä ja vaikuttavat meitä koskeviin päätöksiin. Perinteiseen yksityisyyteen vaikeasti sovitettava sähköinen profiilimme vaikuttaa siihen, miten kykenemme osallistumaan ubiyhteiskuntaan. Sen perusteella päätellään, mikä on kelpoisuutemme eri tarkoituksiin. Profiilin tiedot voivat tulla vastaan vuosienkin jälkeen. Esimerkiksi työnantajat arvioivat niiden avulla sopivuuttamme tulla valituksi työhön tai edetä työssämme.

Yksilöä koskeviin päätöksiin vaikuttavat yhä yleisemmin tapahtumatiedot. Yksilöstä näin saatu kuva on aina vääristynyt, se kätkee todellisen minämme. Jos esimies käyttää hyväkseen alaisensa, kauppias asiakkaansa tai viranomainen kansalaisen arvioinnissa tietoja tämän hiiren klikkailuista tai muista tapahtumista kerättyjä tietoja, arviointi voi johtaa täysin harhaan. Klikkaustiedot eivät välttämättä ole merkittäviä tai usein edes tietoisia mielipiteen ilmauksia tai kannanottoja.

Perinteinen kyselyjen ja rekisterien pohjalta rakennettu tietoprofiili on aina pelkistetty, mutta edustava ja hallittu kuvaus yksilöstä. Tietoverkoissa esitettävä yksilön profiili on vääristyneempi kuin rekistereistä saatu kuva. Verkossa on mahdollista kaunistellakin todellista minää. Yhteisöpalvelujen sivustoilla esitettyjen profiilien avulla pyritään houkuttelemaan sopivia ystäviä itselleen. Ubiikissa ympäristössä rakentuva yksilön tietoprofiili on lähes mielivaltainen. Siellä on vaikea vaikuttaa kuvaan ja sen käyttöön ja ylipäätään edes tietää siitä mitään.

Tunnistusteknologiat ovat yksi ubiympäristön nopeimmin kehittyvistä aloista. Tunnistimet voidaan sijoittaa siten, että asiallisten käyttäjien ja kulkijoiden lisäksi myös asiattomat jättävät niihin jälkiään – yleensä tietämättään. Kehittyneet tunnistustekniikat helpottavat jäljitystä. Ne ovat tehokas ase väärinkäytöksiä vastaan.

Kun ubiympäristössä asioidaan sähköisesti, osapuolten välillä ei ole välitöntä kosketusta. Tunnistettava kansalainen tai asiakas ei kontrolloi tunnistustilannetta, eikä välttämättä tiedä toisesta osapuolesta mitään. Ihminen voi ubiympäristössä navigoida paikasta ja tunnistustilanteesta toiseen, eikä yleensä edes tajua tulleensa tunnistetuksi.

Valvontayhteiskunnan kehittyminen

Valvonta nopeutuu, laajentuu ja yhdentyy

Max Weberin näkemykset kansallisvaltion hallinnon kehityksestä ovat olleet tärkeitä. Hänen mukaansa byrokratian kehityksen avaintekijä on tieto ja sen merkitys hallinnolle. Modernin byrokraattisen valtion kyky hallita ja valvoa perustuu sen kykyyn tietää yhteiskunnasta ja sen kansalaisista.

Valtio tuottaa sosiaalisen, taloudellisen ja teknisen infrastruktuurin kansalaisilleen sekä asettaa sääntöjä ja lakeja niiden käyttämiselle. Hallinto kontrolloi tietojen avulla, miten palveluja tuotetaan, kuka saa käyttää mitäkin palveluja ja kuka pääsee käsiksi mihinkin tietoon.

Kaikenlaiset rekisterit ja muut tietovarastot ovat hallinnolle tärkeitä. Rekisterit on rakennettu palvelemaan erilaisia tarkistuksia palvelujen tuottamisessa, mutta myös rajoitusten ja edellytysten määrittelyssä. Vaikka ihmisistä kerättäisiin tietoja hyvinkin harmittomiin tarkoituksiin, niitä on helppo käyttää myös erimuotoiseen valvontaan. Esimerkiksi puhelujen laskutustietojen avulla seurataan rikoksesta epäiltyjen yhteyksiä.

Valvonta perustui aiemminhankalasti käytettäviin paperiarkistoihin. Nykyaikaisen valvonnan perustana on tietokanta. Käsitettä tieto(kanta)valvonta on käytetty (Clarke, 1988) kuvaamaan tapoja, joilla yhteiskunnat tekniikan avulla ottavat käyttöön tietoon perustuvia valvontamuotoja. Massiivisia määriä tietoja voidaan kerätä ja käyttää tietokannoista paljon nopeammin ja tarkemmin kuin vanhamuotoisia paperiarkistoja.

Tietovalvonnassa ihmisten tekemisiä tarkistetaan automaattisesti. Tällainen on paljon tehokkaampaa ja taloudellisempaa kuin perinteinen valvonta. Clarke (1988) toteaa viitaten orwellilaiseen skenaarioon, että ”siinä esitetty kaksisuuntainen televisio ei ole toteutunut, vaikka se on toteutettavissa. Se ei ole tarpeen, koska tietokantavalvonta on teknisesti ja toiminnallisesti parempi”. Katselun perusteella rahoitettava vuorovaikutteinen digi-televisio olisi viihteellinen kevytversio Ison Veljen telescreenistä. Tänään valvonta on nimenomaan tietovalvontaa.

Tietokantoihin pohjautuva valvonta ruokkii itse itseään. Mitä enemmän ja merkittävämpiä tietoja kirjataan rekistereihin, sitä tarkoituksenmukaisempaa on perustaa valvonta suoriin tarkistuksiin niistä. Vaikka valvonnan osapuolten kontaktit lisääntyvät, valvontaa koskeva tieto

löytyy vaivattomammin hakemalla tietokannasta kuin kysymällä henkilöltä itseltään. Tämä toimintatapa näyttäisi olevan toteutumassa hallinnon sähköisen asioinnin ympäristössä, jossa ”monet asiat voidaan hoitaa asiakkaan puolesta niiden tietojen avulla, jotka viranomaisilla jo on eri tietojärjestelmissä” (VM, 2007).

Tietovalvonnan tärkeä ominaisuus on mahdollisuus koota tietoja eri lähteistä. Eri järjestelmistä kerätyt tiedot voidaan yhdistää tuottamaan uutta ja valvonnan kannalta arvokasta tietoa. Yhdistelyn avulla on mahdollista tunnistaa etsittäviä tapahtumia ja henkilöitä.

Tietovalvonnan käytännössä korostuu yksi ominaisuus. Huolimatta ehkä hyvinkin hajautetusta rakenteesta tietokannat muodostavat toiminnallisesti yhtenäisen kokonaisuuden.

Tietojärjestelmiä rakennettaessa, niiltä edellytetään nykyisellään keskinäistä yhteentoimivuutta, jota tukee eri teknologioiden kasvava konvergenssi (yhdentyminen). Eri järjestelmien yhteiskäyttöä ja yksilöön liittyvien tietojen helppoa kokoamista varten tarvitaan yleinen ja yhdenmukainen avain, kuten sähköinen identiteetti. Se lisää tietovalvonnan tehokkuutta eri tarkoituksissa ja kuten työpaikoilla, virastoissa, kaupoissa, pankeissa, rajan ylityksissä, liikennevälineissä.

Jotta tietoja kyetään käyttämään tehokkaasti palveluihin ja valvontaan, tiedot on voitava yhdistää ihmisiin ja heidän identiteetteihinsä. Varsinkin tietoverkoissa järjestelmien ja palvelujen käyttäjien kontrollin tavoitteeksi on tullut identiteettien hallinta. Sillä määritellään, kuka pääsee käsiksi käyttäjien identiteetteihin ja niihin liitettäviin tietoihin.

Riskien hallinnan ruokahalu kasvaa

Valtion keskeisenä tehtävänä on ollut tuottaa hyvinvointipalveluja kansalaisille. Viime vuosina hyvinvointiajattelu on alkanut korvautua riskiajattelulla. Positiivisten sosiaalisten tavoitteiden sijaan olemme yhä enemmän huolissaan kansalaisten aiheuttamista riskeistä.

Palvelujen tuottamista on alettu katsoa riskien hallinnan näkökulmasta. Riskeinä ovat palveluja käyttävät ihmiset. Mitä enemmän tiedetään ihmisestä, sitä paremmin kyetään hallitsemaan hänen palvelujen käyttöään ja eliminoimaan häneen liittyvät riskit. Riskien karttamisen tiedollinen ruokahalu kasvaa jatkuvasti.

Organisaatiot rakentavat valvontajärjestelmiä ja luovat asenneilmastoa, missä kansalaiset, työntekijät ja asiakkaat saavat ymmärtää, että heidän toimiaan on seurattava. Valtio luokittelee kansalaisia riskien perusteella ja etsii ihmisiä, jotka toimivat poikkeavasti ja rikkovat sääntö-

jä. Yritykset rakentavat valvontakäytäntöjä hallitakseen työntekijöitään heidän riskiensä perusteella. Työnantajat seuraavat työntekijöiden tietokoneen näppäilyjä, viestintää ja verkon käyttöä.

Aiemmin valtion vallankäytön tärkeä väline oli salainen tiedustelutieto. Tällaisen vallan metafora oli orwellilainen valtio, missä totalitaarinen kontrolli perustui valtion tiedon monopoliin. Ylhäältä käsin pyrittiin salaisen tiedon avulla valvomaan alamaisia.

Tälle vuosisadalle orwellilainen valtio on harhaanjohtava malli valtion vallan ja valvonnan rakenteesta ja tiedon roolista valvonnassa. Orwell ei kauhukuvitelmissaan osannut ennustaa tietokoneiden, tietoverkkojen ja tietojenkäsittelyn digitalisoinnin seurauksia. Ne ovat laajentaneet dramaattisesti mahdollisuuksia kerätä ja käyttää tietoja byrokraattisen kontrollin ohella kaikenlaiseen seurantaan – myös itse vallanpitäjien valvontaan. Kaikkialla läsnä oleva tietojenkäsittely pakottaa rakentamaan vallan ja valvonnan rakenteet uudelleen.

Viestintää ja verkonkäyttöä valvotaan hyvinkin eri tasoilla. Yhdysvaltain ja sen liittolaisten ylläpitämä Echelon-valvontajärjestelmä suodattaa rutiininomaisesti kaikkia nykyaikaisen viestinnän ja verkonkäytön muotoja. Yhdysvaltain turvallisuusviranomaiset seulovat kansainvälisten selvitysjärjestelmien kautta kulkevaa rahaliikennettä. Ruotsissa ehdotetaan sähköpostiliikenteen yleistä seurantaa. Suomessa työnantajat ovat saamassa oikeuden seurata tarvittaessa työntekijöiden sähköpostiliikennettä.

Tiedonkeruu ja valvonta

Ihmisten tekemisten seuraaminen on yhtä vanhaa kuin ihmisyys itse. Kun valvontaa harjoitettiin pienissä yhteisöissä, asutuksissa ja kylissä, niissä pantiin merkille kaikki poikkeava ja epätavallinen käyttäytyminen. Jos naapurien jatkuva seuranta tuntui ahdistavalta, sitä oli mahdollista paeta suurempiin kaupunkeihin. Siellä asukkaiden suuri määrä ja liikkuvuus teki lopun perinteisestä naapurivalvonnasta. Anonyymina eläminen on pitkään ollut kaupunkimaisen elämänmuodon avainpiirre.

Automaattisen tietojenkäsittelyn myötä tietokoneet ovat saaneet valvojan tehtävän. Niiden avulla on alettu rekisteröidä ja säilyttää tietoja tunnistettujen ihmisten päivittäisistä rutiineista. Kiinnostavia ovat ennen kaikkea poikkeavat ja epänormaalit käyttäytymiset.

Ubiikkiyhteiskunnassa palataan tältä osin pikkukylän naapurivalvontaan. Valvovina silminä ja korvina eivät kuitenkaan ole naapurit seinän takaa, vaan näkymättömät tietojärjestelmät ja niiden tuntemattomat isännät. Uuden valvonnan keskeinen seuraus tulee olemaan anonymiteetin häviäminen.

Kuulemme jatkuvasti varoituksia, että olemme vähitellen liukumassa valvontayhteiskunnaksi. Valvontayhteiskunnasta puhuttaessa ajatellaan usein jonkinlaista ”Ison Veljen” johtamaa totalitaarista poliisivaltiota, jossa jokin yksittäinen taho (Iso Veli) on valvonnan takana. Totuus on, että elämme jo yhteiskunnassa, joka valvoo monilla tavoilla tarkoin kansalaisiaan.

Valvonnan kehitystä arvioitaessa ratkaisevaa on se, mitä valvonnan välineet ja käytännöt mahdollistavat – ei vain toteutunut valvonta. Valvontamahdollisuudet ovat eri kriteereillä mitattuna tehostuneet kehittyneissä yhteiskunnissa erityisesti viimeisen kolmen vuosikymmenen aikana. Suomi on tässä yksi edelläkävijöistä maailmassa.

Tietojen määrä rekistereissä on kasvanut valtavasti. Samalla tietojen käyttötavat ja -tarkoitukset ovat laajentuneet ja monipuolistuneet. Tämä johtuu viime vuosikymmenien verkottumisesta ja tietovarastojen muokkaus- ja analysointivälineiden kehityksestä. Esimerkiksi

- viranomaiset rekisteröivät tekemisemme tarkoin virastoissa, laitoksissa paikan päällä ja verkon kautta kotona, kaduilla ja teillä
- jos olemme väärään aikaan väärässä paikassa ja väärässä seurassa, joudumme herkästi viranomaisten seurantaan
- kun matkustamme lentokoneella ulkomaille, meitä seurataan ja meidät on väritetty riskiprofiilimme perusteella ennen kuin ehdimme lähteä kotoa. Jatkossa älykkäät liikennejärjestelmät seuraavat meitä ajantasaisesti, kun liikumme autolla
- meidän on jatkuvasti osoitettava, keitä olemme ja todistettava, että olemme oikeutettuja tekemään tai saamaan sen, mitä haluamme
- kulutustottumuksemme on kauppiaan tiedossa. Kauppaketju tietää jääkaappimme sisällön, mitä meiltä puuttuu ja mitä meidän pitäisi haluta.
- raha- ja maksutapahtumistamme ovat kiinnostuneita kotimaisten pankkien ohella ulkomaiset tiedusteluviranomaiset. Tiedot siirretyistä euroistamme kiertävät valtamerten yli.
- viestintämme ja verkonkäyttömme ovat tarkassa seulonnassa. Kotimaisten viranomaisten ja työnantajien lisäksi niistä ovat kiinnostuneet kansainväliset tiedusteluviranomaiset.
- työntekomme voi olla tarkkaan rekisteröityä, tapahtuipa se työhuoneessa tai kesämökin laiturilla. Työnantajia yhä useammin kiinnostaa myös asenteemme ja ajattelumme. Jotkut työnantajat haluavat seurata surfailujammekin.

Henkilötietoja on Kelan, väestöviranomaisten, verottajan ja sosiaali- ja terveysviranomaisten rekistereissä, kuntien, pankkien ja vakuutuslaitosten tai kaupan organisaatioiden rekistereissä valtava määrä. Kun näitä tietoja käytetään kontrolloimaan ihmisten edellytyksiä ja oikeuksia kansalaisina, asukkaina, asiakkaina ja työntekijöinä, voidaan puhua myös valvonnasta.

Rekistereissä olevien tietojen lisäksi huomioon on otettava se, kuinka teknologia mahdollistaa tietojen käytön valvontaan, minkälainen merkitys ihmisten tunnistuksilla ja rekisteröinneillä on heidän elämäänsä ja mikä on yhteiskunnan poliittinen tahto valvoa. Nämä kaikki seikat osaltaan perustelevat sitä, että suomalaista yhteiskuntaa voidaan kutsua valvontayhteiskunnaksi.

Uuden teknologian sivuvaikutukset

Kansalaisen tekemiset ja toiminnot ovat monilta osin jo jatkuvassa kontrollissa. Valvonta ei modernissa valtiossa suinkaan ole yksiselitteisesti negatiivista. Valtaosa valvonnasta on perusteltua. Pyrkimyksenä voi olla esimerkiksi sosiaali-, terveys- koulutus- tai liikennepalvelujen tuottamisen ja käyttämisen tehokkuus, taloudellisuus, turvallisuus sekä kohtuullisuus ja yhdenvertaisuus, jotka ovat tärkeitä kansalaisen arvoja ja intressejä.

Osa valvonnasta pyrkii kontrolloimaan ja rajoittamaan toimintaa kansalaisen tietämättä tai ilman hänen suostumustaan. Kansalainen ei läheskään aina tiedä tai ymmärrä, mitä hänen tiedoilleen tapahtuu ja mihin niitä käytetään. Yleensä hänellä ei ole syytä huolestua tästä. Mutta jos asiat alkavat mennä huonosti, tapahtuu vääriä asioita tai olosuhteet ovat epäsuotuisia, hänen tietojaan voidaan käyttää tavoilla, joita hän ei hyväksy.

Teknologian, yhteiskunnan ja valvonnan vuorovaikutuksesta on esitetty hyvinkin erilaisia näkemyksiä. On helppo yliarvioida tietokoneiden vaikutuksia valvontaan. Kiistatonta kuitenkin on, että teknologia mahdollistaa tehokkaan valvonnan ja tekee puuttumisen ihmisten elämään helpoksi.

Kansalaisten massamuotoinen valvonta ei ole uutta. Vasta tietokoneet, tietoverkot ja tietokannat ovat kuitenkin mahdollistaneet kansalaisten jatkuvan, syvälle tunkeutuvan ja kattavan valvonnan. Siirtymä fyysisestä valvonnasta sähköiseen on ennen kaikkea yksityisyyden kannalta dramaattinen. On esitetty, että maailma ilman yksityisyyttä on jo teknisesti mahdollinen.

Kansalaiset ovat tietokantoihin perustuvan valvonnan kohteina juuri tietoteknisesti kehittyneissä maissa, kuten Suomessa. Keskiverto venäläinen tai kiinalainen saa olla hyvin rauhassa sähköiseltä valvonnalta. Tosin nämäkin maat kurovat kehittyneiden maiden etumatkaa nopeasti umpeen. Kehittyneiden valvontateknologioiden käyttöönotto näissä maissa on erityisen huolestuttavaa siksi, että niissä kansalaisten ihmisoikeuksien toteutumisessa on nykyiselläänkin ongelmia.

Tietoliikenteen kehitys on lisännyt mahdollisuuksia hoitaa hallinnollisia ja muitakin asioita tietoverkkojen välityksellä. Sähköinen asiakirja on korvaamassa perinteisen paperiasiakirjan. Sähköinen asiointimahdollisuus merkitsee asioinnin tehostumista. Esimerkiksi kansalaiselle avattava asiointitili ”nähdään tärkeänä askeleena julkishallinnon sähköisen asioinnin kehittämisessä” (VM, 2007). Se merkitsisi myös asioijan kattavampaa seurantaa. Keskitetty asiointitili voisi kertoa kansalaisen koko asiointihistorian eri tahoille.

Kansalaisten riippuvuus sähköisistä tunnistuskäytännöistä on kasvanut jatkuvasti. Suomalaisten kukkaroista ja taskuista löytyy iso kirjo kortteja ja muita tunnistusvälineitä. On esitetty pelkoja, että sähköisistä tunnistusjärjestelmistä, ennen kaikkea sähköisestä identiteetistä tulee yhteiskunnalle tehokas keino kontrolloida kansalaisiaan. Sähköinen identifiointi sopii ihanteellisesti valvontayhteiskunnan toimenkuvaan.

Ubiyhteiskunnassa tilanteet, joissa valvojat ja valvottavat kohtaavat lisääntyvät tavattomasti. Lisäksi yksittäiset kohtaamiset ovat hyvin huomaamattomia. Asioijan tunnistusmahdollisuus moninkertaistaa rekisteröitävien kontaktien määrän verrattuna tavanomaiseen rekisterinpitoon, perinteisistä fyysisistä asiointitavoista puhumattakaan.

Mitä tekivät ihmiset, kun valvontayhteiskunnasta päätettiin? Valvontayhteiskunta ei ole minkään salaliiton aikaansaannos. Se on tullut hitaasti ja huomaamatta, monien tekijöiden ennakoimattomanakin yhdistelmänä. Se on tulos teknologisesta kehityksestä, poliittisista päätöksistä ja sosiaalisesta muutoksesta. Yhteiskunnallisen valvonnan lisäämiselle on saatu oikeutusta yksittäisistä tapahtumistakin, kuten New Yorkin, Madridin ja Lontoon terrori-iskuista.

Kameroiden ja satelliittien valvova silmä

Kameravalvonta on yksi nopeimmin kasvavista valvonnan muodoista. Se on tullut mitä erilaisimpien tilojen ja alueiden valvontaan: virastoihin ja laitoksiin, asiakaspalvelutiloihin, ostoskeskuksiin ja kauppoihin sekä katujen, teiden ja torien varsille. Suomalainen kaupunkitila on muut-

tunut sellaiseksi, että siinä liikkuessaan ihminen on suuren osan ajasta seurattavissa jostakin monitorista ja hänen kulkemisensa ja tekemisensä tallentuvat videonauhalle.

Uuden teknologian avulla kameroilla nähdään entistä kauemmaksi ja laajemmalle, hämärämmässä ja tarkemmin. Videovalvonnan innovaatiot ovat tehneet valvonnasta pysyvää ja kattavaa. Hahmontunnistus ja tietojen digitaalinen käsittely ja siirtely tarjoavat kameravalvonnalle joustavaa mukautumista.

Paikallista järjestyksenpitoa voidaan laajentaa rajojen yli tapahtuvaan yksilöjen tunnistukseen, paikannukseen ja seurantaan. Mitä kauemmin kuvia säilytetään ja tarkemmin niitä indeksoidaan sen mukaan, mitä ne esittävät, sitä paremmin kuvia voidaan hakea ja yhdistää etsittäviin henkilöprofiileihin.

Jeremy Bentham esitteli kaksi vuosisataa sitten ajatuksensa Panopticonina tunnetusta vankilasta. Hänen vankila-kuvitelmassaan alueen keskellä oli valvontatorni ja reunoilla kehän muotoinen rakennus. Valvontatornista oli näkymä ympäröivän rakennuksen selleihin.

Vankilan asukkeja voitaisiin seurata jatkuvasti. He eivät voisi tietää, olisivatko silmällä pidettävinä milläkin hetkellä. Heidän olisi kuitenkin viisasta lähteä siitä, että heitä seurattaisiin jatkuvasti.

Bentham näki Panopticoninsa uudenlaisena mieltä hallitsevana valtana, jonka kapasiteetti ylittää tähänastiset esimerkit vallankäytöstä – ”as a new mode of obtaining power of mind over mind, in a quantity hitherto without example” (1995). Vaikka Benthamin suunnitelmaa ei toteutettu, hänen ajattelunsa innoittamana on rakennettu useita laitoksia.

Panopticonista on tullut täydellisen valvonnan vertauskuva. Sellaisena se on erittäin ajankohtainen tämän päivän ubiikissa valvontaympäristössä. Sähköisten jälkien tallentuminen lukemattomiin paikkoihin luo aidon panoptisen valvonnan mukaisesti epävarmuutta ihmisissä. He eivät tiedä näistä käytännöistä ja vaikka tietäisivätkin, he eivät kykene niihin vaikuttamaan.

Uusi Panopticon on kuvitelma jatkuvasta valvonnasta. Ihmiset eivät välttämättä ole aina valvonnan alaisina. Heidän on kuitenkin perusteltua olettaa, että ovat. Kun ihmiset olettavat, että heitä seurataan jatkuvasti, he sisäistävät säännöt ja normit ja elävät kuuliaisesti ja toivotulla tavalla. Juuri tähän jatkuvan panoptisen valvonnan pelkoon perustuu satelliittipohjainen liikennevalvonta. Samaan vaikutukseen pohjautuvat myös ajatukset työntekijöiden sähköisen viestinnän seuraamisesta.

Jo Bentham lähti siitä, että panoptista valvontaa voi harjoittaa muis-

sakin laitoksissa kuin vankilassa. Laitokset, joihin hän uskoi panoptisten periaatteiden soveltuvan, perustuisivat jonkin asteiseen pakkoon. Ranskalaisen filosofin Foucault'n mielestä panoptista valvontaa ei pidä rajoittaa yhteiskunnasta eristettyihin laitoksiin ja paikkoihin. Hän näki panoptisen valvonnan rakennetun yhteiskuntaan sisään, jolloin koko yhteiskunta on vankila.

Kameravalvonta ja mikä tahansa seurannan sähköinen muoto on kehittynyt panoptisen valvonnan periaatteiden mukaiseksi epäpersoonalliseksi ja etäiseksi silmälläpidoksi. Kontrolli on kasvotonta, valvojan ja valvottavan välillä ei ole suoraa kontaktia. Valvottava ei tiedä, kuka häntä valvoo, missä ja miten valvotaan vai valvooko ylipäätään kukaan.

Panoptinen yhteiskunta

Visiot arjen tietoyhteiskunnasta sisältävät sen, että pieniä mikrosiruja, langattomia viestimiä ja muita tunnistimia sijoitetaan kaikkiin mahdollisiin kohteisiin. Näiden avulla rakennetaan ”älykkäitä” ympäristöjä, koteja ja autoja, joissa tietokoneet häviävät seiniin, rakenteisiin ja kaikkiin esineisiin. Tarkoituksena on, että ne auttavat taustalla vapauttamalla meidät monista ikävistä arjen rutiineista.

”Älykkäät” esineet ja rakenteet havainnoivat ympäristöään ja siinä liikkuvia. Ne ovat vuorovaikutuksessa ”älykkäitä” esineitä kantavien älykkäiksi itsensä kokevien ihmisten kanssa. Tällaisessa maailmassa on mahdollista rekisteröidä kaikki toimintamme, liikkeemme ja ilmaisujammekin.

Tämän teknologisen edistyksen näkymänä on täydellinen valvontayhteiskunta, jossa suurinta osaa elämästämme seurataan lukemattomilla kameroilla, paikannuslaitteilla ja muilla tunnistimilla. Älykkäiden laitteiden avulla kyetään ”lukemaan ajatuksiamme” ja ennakoimaan tulevaa käytöstämme sekä varautumaan siihen.

Ubiikkiyhteiskunnalla on valvontamahdollisuuksia, joista entisaikojen todelliset ja kuvitteelliset Isot Veljet ovat voineet vain haaveilla. Äärimmillään hallinto voisi kerätä tietoja jokaisen kansalaisen kaikista tapahtumista ja liikkeistä ja viesteistä. Tällaisessa maailmassa tuskin mikään tapahtuma jäisi paljastumatta ja merkittävä teko vaille seurauksia.

Valvonnan teknologia on kameroiden ja muiden, yleensä näkymättömien tunnistimien avulla tehnyt kaupunkiemme tiloista ja laitoksista sekä koko yhteiskunnastakin suunnattomia sähköisiä panoptikoneja. Nyt selleissä on vankien lisäksi potilaita, oppilaita, työntekijöitä ja asiakkaita ja ylipäätään ihmisiä, jotka liikkuvat julkisissa ja yksityisissäkin

tiloissa tai asioivat verkossa. Benthamin täydelliseksi kuvittelema valvonta on tuotu vankilasta ulos yhteiskuntaan.

Benthamin panoptisen valvonnan ja ubiyhteiskunnan valvonnan keskeisin eroavuus on kompleksisuus. Yhteiskunta on paljon monimutkaisempi valvottava. Se on myös vaikeammin ymmärrettävä kuin vankila tai muu suljettu laitos. Vankilassa valvottava ymmärtää tilanteensa ja hänen on helppo sopeuttaa käytöstään haluamallaan tavalla. Ubiikin maailman valvonnan tilanteiden ja tietojen määrä on liian suuri, jotta käyttäjä ymmärtäisi ja kykenisi kontrolloimaan niitä.

Uudet tekniikat tarjoavat mahdollisuuden alueellisesti kattavaan valvontaan koko yhteiskunnan tasolla. Tietojen säilytysvelvollisuus, minkä teletunnistetietoihin liittyvä lainsäädäntö tuo mukanaan, tekee valvonnasta ajallisestikin kattavan. Teleliikenteen ja verkon käyttötietojen säilytysvelvollisuuden myötä käytön seurannan vaikutukset yksityisyydelle kasvavat dramaattisesti. Enää ei paljastu vain yksittäisiä tapahtumia tai sijainteja, vaan on mahdollista kirjoittaa kattavaa tapahtuma- ja liikkumishistoriaa.

Ubiikissa valvonnassa käytetään hyväksi pelkoja, omasta, lasten ja vanhusten ja muidenkin tärkeiden ihmisten ja asioiden turvallisuudesta. Sen toimintaan on rakentunut itseään ruokkivaa dynamiikkaa. Ilman valvonnan suojaa olevien alueiden, tilojen, ihmisten ja toimintojen pelätään joutuvan väärinkäytösten, ilkivallan ja rikollisuuden kohteiksi. Kun kamera puuttuu jostain tilasta, rikolliset siirtyvät sinne sieltä, missä kameroita jo on. Sen jälkeen kameroita halutaan sinne, mistä ne puuttuvat ja seurantalaitteita niille, joilta ne puuttuvat.

Pikkuveljet ja hajautettu valvonta

Iso Veli -kauhukuvat ovat aina herättäneet pelkoa. Kuvitelma kaiken näkevästä silmästä on ollut synonyymi valtion harjoittamalle tukahduttavalle valvonnalle. Tänään silmän ei välttämättä tarvitse kuulua valtiovallalle. Ironista on, että isovelivaltion valvonnan läpitunkevuus on toteutunut paljon tehokkaammin yksityisellä kuin julkisella sektorilla.

Onko niin, että olemme varautuneet vastustamaan vain Ison Veljen tulemista? Sen sijaan emme ole huomanneet lukemattomien pikkuveljien hiipimistä elämäämme ja yksityisyyteemme. On helpompi vastustaa keskitettyä valvontakeskusta, yhtä Ison Veljen silmäparia kuin lukemattomia, hajallaan olevia ja ehkä kilpaileviakin silmäpareja. Siitä huolimatta, että nämä lukemattomat silmäparit ovat paljon kattavampia ja tunkeutuvampia kuin keskitetty ja kaikkivaltias Iso Veli.

Ubiyhteiskunnan pikkuveljet keräävät tietoja ihmisten elämästä. Pikkuveljet ovat tietävinään, mitä ihmisten pitäisi haluta. Heillä on välineet arvailla ja päätellä ihmisten motiiveja ja aikomuksia. Ubiyhteiskunnan valvonnan vahvuus on siinäkin, että ihmiset vapaaehtoisesti suostuvat osallistumaan valvontaansa, koska he kokevat saavansa siitä hyötyjä. Hyödyt ovat yleensä konkreettisia, kun taas haitat, esimerkiksi yksityisyyden menetys, ovat enimmäkseen hyvin abstrakteja.

Uusi valvonta välttää edeltäjiensä raakuudet. Tämän päivän valvonta on hienovaraista ja suostuttelevaa. Kun panoptinen katse kohdistetaan kuluttajaan, se pyrkii ymmärtämään hänen tarpeitaan ja auttamaan niiden toteuttamisessa. Mitä enemmän kauppiaat tietävät asiakkaistaan, sitä paremmin he voivat palvella näitä. Osallistuva, suostutteleva ja aitoihin hyötyihin perustuva valvonta on paljon vaikuttavampi kuin pakottamiseen perustuva valvonta.

Ubiyhteiskunnan porkkana on hyödykkeiden ja palvelujen tuottama mielihyvä. Toisaalta sen tehokas pakote on pois sulkeminen ja ulkopuolelle joutuminen. Orwellin visiossa toisinajattelevat eivät halunneet mitään enempää kuin piiloutua Ison Veljen katseelta ja paeta jonnekin pois. He eivät voineet, koska sellaista mahdollisuutta ei ollut. Winston Smithkin ”oppi” lopulta hyväksymään valvontansa ja rakastamaan Isoa Veljeä.

Kun Orwell kuvitteli Ison Veljensä, hän näki mallina oman aikansa poliittiset diktaattorit. Hän oletti, että teknologia taipuisi palvelemaan nimenomaan heitä. Hän oli väärässä.

Ubiteknologia ja osallistuva valvonta ovat tehneet Ison Veljen vanhanaikaiseksi. Eräs uuden teknologian keskeisistä vaikutuksista valvontaan on ollut juuri keskitetyn valvonnan tarpeen vähentyminen. Ihmiset ovat mukana, usein tietämättään, rakentamassa valvontayhteiskuntaa. Pikku veli on henkisesti hajautettu meihin kaikkiin – valvoja on siirtänyt tehtäviään valvottavalle.

Onko ubimaailmassa yksityisyyttä?

Yksityisyyden vaihtokauppa

Arjen tietoyhteiskunnassa tai ubiikkiteknologian yhteiskunnassa kansalaisen kannalta keskeinen kysymys on, mihin suuntaan yksityisyys kehittyy. Onko se kaventunut, pysynyt ennallaan vai peräti parantunut viime vuosina?

Sen kokeminen, mikä on hyväksyttävää puuttumista yksityiselämään ja mikä ei, on subjektiivinen tuntemus, joka vaihtelee ajan, paikan ja yhteisön mukaan. Sen perusteella on vaikea arvioida yksityisyyden kehitystä.

Mitä tulee ajatella kaupan kanta-asiakaskorteista, jotka henkilö on vapaaehtoisesti ottanut käyttöönsä. Niiden avulla kaupat rekisteröivät hänen ostoksiaan, seuraavat hänen kulutustottumuksiaan ja profiloivat hänet hyväksi tai vähemmän hyväksi asiakkaaksi.

Kiistatta asiakkaan yksityisyyteen on puututtu, toisaalta tämä on toteutunut sääntöjen mukaan. Asiakas ei ehkä koe yksityisyytensä kaventuneen. Entä milloin profilointi ylipäätään loukkaa yksityisyyttä, kun ihmiset yhä yleisemmin profiloivat itseään verkon yhteisöpalvelujen sivustoilla.

Tarkoituksenmukaisempaa on arvioida, miten yksilön yksityisyyden piiri ja siihen kuuluvat asiat ja ilmiöt ovat muuttuneet erityisesti valvonnan suhteen. Ovatko ne pienentyneet, pysyneet ennallaan vai kasvaneet? Tätä kehitystä on syytä arvioida siitä riippumatta, onko se tapahtunut yksilön tieten vai tietämättä, tahtoen vai tahtomatta tai miten yksilö asian on kokenut.

Westin (1967) on määritellyt yksityisyyden suojan ”yksilön oikeudeksi päättää itse, missä, kuinka ja milloin häntä koskevia tietoja käsitellään”. Tässä pidetään tärkeämpänä arvioida oikeuden asemesta yksilön kykyä kontrolloida itseään koskevien tietojen käsittelyä ja sen osalta mahdollisuutta olla rauhassa muiden asiattomalta puuttumiselta. Kun tiedonkeruu on tullut yhä vähemmän näkyväksi, ei subjektiivinen kokemus itsemääräämisoikeuden toteutumisesta vastaa enää todellisuutta. Tietoyhteiskuntakehityksen myötä oikeus ja kyky erkanevat koko ajan kauemmaksi toisistaan.

Älykkäästä elinympäristöstä maksettava hinta on yksityisyyden menetys. Älykkäät maksu- ja asiakaskortit tarjoavat parempaa palvelua, mutta samat kortit tarjoavat tietoja pankeille ja kaupalle. Samalla teknologialla, joka auttaa rahalaitoksia alentamaan luottokorttitappioita, voidaan valvoa kortin haltijan elämää. Teknologia, joka tarjoaa asiakkaalle vaivattoman maksutavan, auttaa myös rakentamaan profiilia asiakkaan ostoksista, mieltymyksistä ja mielipiteistä.

Sairaushistoriamme muovikortilla pelastaa ehkä henkemme. Kuka silloin uskaltaa kieltäytyä kortista. Samalla kortilla, jolla hoituvat reseptit ja lääkkeet, kyetään profiloimaan ja hinnoittelemaan vakuutetut oikein. Kansallinen DNA-rekisteri parantaa mahdollisuuksia paljastaa rikolli-

sia, mutta se voisi myös vaikuttaa vakuutuksen tai työpaikan saamiseen. Teknologia, jolla työntekijä kuittaa päivittäisen lounaansa, kertoo työnantajalle hänen ajankäyttönsä ja kulkemisensa. Samalta luukulta, jolta yhteiskunta tarjoaa palveluja, voidaan arvioida kansalaisen kelpoisuutta.

Valvonta ja palvelut kytkeytyvät yhteen. Kun lisäämme valvontakameroita, saamme turvallisempia ostoskeskuksia ja katuja. Paikantava siru paljastaa automme anastajan. Ketä silloin haittaa jatkuva jäljitys? Sama teknologia, jolla vähennetään liikenneruuhkia, kertoo autoilijan liikkumiset. Älykäs puhelin tarjoaa lisää palveluja, mutta samalla se voi tarjota lisää tietoja operaattorin lisäksi esimerkiksi työnantajalle, poliisille, kauppiaille tai pankeille. Televiestintäni ja tietoverkkojen käyttöni seuranta turvaa maailmaa terroristeilta.

Anonyymin asioinnin loppu

Käyttäjien yksityisyyden suojaamiseksi on ehdotettu, että heillä olisi mahdollisuus päättää, milloin haluavat tulla tunnistetuiksi ja siten osoittaa, miten haluavat tietojaan käytettävän. Mutta kuinka käyttäjät kykenevät valitsemaan tunnistuksiaan, tietojen käyttöjään ja siten päättää yksityisyytensä rajoista, jos he eivät ubimaailmassa tiedä näistä mitään? Esitetty vuorovaikutteisuus ei takaa aitoa mahdollisuutta vaikuttaa yksityisyyteensä. Lisäksi ihmisillä on harvoin aikaa ja energiaa tai aina edes riittävää motivaatiota selvittää tällaisia asioita.

Pyrkimyksenä on tehdä sähköinen anonymiteetti käytännössä mahdottomaksi antamalla kaikille tietokoneille ja muille tietoja käsitteleville laitteille ainutkertainen identifiointinumero (ip-osoite). Yksityisyyden kannalta tilanne tulee erityisen polttavaksi siinä vaiheessa, kun yksilöiviä siruja (esim. sirukortit) luetaan laitteessa. Silloin laitteiden tunnusta voidaan käyttää tunnistamaan sekä laite että sen käyttäjät. Jokainen tieto, jonka laitteen käyttäjä lähettää tai vastaanottaa sähköisesti, sisältää käyttäjän tunnistavan jäljen.

Ubiikki tietojenkäsittely peittää yhä useamman ihmisen arkea yhä kattavammin. Yhteiskunnat, organisaatiot ja ihmiset tulevat siitä yhä riippuvaisemmiksi. Sitä enemmän lukkiudutaan ajatukseen, että teknologia on myös paras keino pelastaa yksityisyys, mikä lisää entisestään riippuvuutta teknologiasta. Yksityisyyden kannalta uuden teknologian keskeinen paradoksi on, että vaikka se antaa teknologian käyttäjille keinoja suojatakin yksityisyyttään, samalla se altistaa heidät tiukemmalle valvonnalle.

Vaikka käytettävissä on yksityisyyttä tukevia teknologisia ratkaisuja, ”parempi teknologia” ei pelasta yksityisyyttä. Uusien palvelujen edellyttämät teknologiat, joissa edellytetään käyttäjien tunnistautumista, sisältävät useimmiten myös käyttäjien valvonnan työkalut. Ubiteknologioiden käyttöönoton myötä valvonnan henki on päästetty pullosta ulos. Hallituksilla ei ole riittävää kykyä kontrolloida teknologioiden käyttöä eikä edes tahtoa pistää henkeä takaisin pulloon.

Yksityisyyden suojaa esitetään ubiajattelussa vanhahtavana, pian muut kuin yksityisyyden radikaaleimmat kummajaiset uiskentelevat kultakaloina tietoakvaariossa. Yksityisyyden suojaa ja varsinkin halua esiintyä anonyymisti pidetään myös epäilyttävänä. Rehellisen ihmisen ei tarvitse pelätä tietotekniikan tarjoamia mahdollisuuksia. Mutta ketkä ovat niitä, joilla ei ole mitään salattavaa? Entä mitä tapahtuu meille, jotka haluamme pitää henkilökohtaiset asiat itsellämme?

Ubiikki kaventaa yksityisyyden

Yksityisyys ei juhlapuheista huolimatta ole merkittävä poliittinen asia ja sitä on abstraktina asiana vaikea puolustaa. Yksityisyydellä on eri intressien punninnassa se arvo, mikä jää konkreettisempien hyötyjen jälkeen. The Economist-lehden (1999) mukaan on liian myöhäistä kysyä, halutaanko lisää yksityisyyttä vai valvontaa. On epätodennäköistä, että löydetään enää yksityisyyden kannalta tyydyttävää ratkaisua sen ja ubiyhteiskunnan voimistaman valvonnan välillä. Valittavana on lehden mukaan yksityisyyden hallittu tai hallitsematon alasajo.

Ennusteet yksityisyydelle ovat siis lohduttomia. Kaikkinaiset yritykset peruuttaa ubiyhteiskunnan tunkeutumista yksityisyyteen ovat tuomittuja epäonnistumaan. Useimmat ihmiset tulevat 20 vuoden päästä havaitsemaan, että tänään taattuna pidetty yksityisyys tulee olemaan yhtä vaikeasti tavoitettava, kuin 1970-luvulla vallinnut yksityisyys nyt näyttää olevan.

Yksityisyys on tuomittu samoista syistä kuin se on rapautunutkin viimeiset vuosikymmenet. Syynä ovat ennen kaikkea yksityisyyden säilyttämisen vastapainoksi asetetut ubiyhteiskunnan lupaukset. Ellei yhteiskunta kollektiivisesti kieltäydy näistä lupauksista, mikä näyttää kaikkein epätodennäköisimmältä ratkaisulta, yksityisyyden säilyttämistä koskevat keskustelut käyvät yhä epätoivoisemmiksi. Ihmisten on syytä totuttautua ajatukseen, että heillä ei välttämättä ole mitään yksityisyyttä.

Ubimaailmassa oikeus päättää tietojensa käsittelystä ja saada olla rauhassa toteutuu harvoin. Valvonta riisuu yksilöt yhä läpinäkyvämmiksi.

Ubiikkiympäristö kutistaa olemattomaksi tilat ja alueet, joihin ihmisillä on aiemmin ollut mahdollisuus vetäytyä yksityisyyteen. Edes jääminen kotiin ei pelasta meitä valvonnalta. Teknologia voi seurata kaikkea sähköistä viestintäämme, verkonkäyttöämme ja liikkumistamme.

Useille ihmisille yksityisyydestä huolehtiminen ei ole tärkeää, kun muita intressejä on vaa'assa. Esimerkiksi verkon yhteisöpalvelujen myötä meille kasvaa sukupolvi, jonka edustajat eivät ole huolissaan, vaikka heidän elämänsä koottaisiin kaikkien nähtäville palvelujen sivustoille. Valtaosa Facebook-palvelun käyttäjistä ei tutkimuksen mukaan muuta oletuksena olevia yksityisyyden asetuksia, jotka antavat vapaat mahdollisuudet katsella profiileja ja käyttää niissä esitettyjä tietoja.

Asennetta kuvastaa hyvin myös Sun Microsystemsin johtajan, Scott McNealyn, tokaisu ”you have zero privacy anyway, get over it” (WIRED, 1999). On esitetty myös ajatus, että yksityisyys on maailman mittakaavassa ylellisyyttä ja ihmisten pitäisi keskittää tarmonsa köyhyyden ja eriarvoisuuden poistamiseen. Niiden rinnalla puuttuva yksityisyys on vähäinen ongelma.

Yksityisyyden hinta tulee nousemaan. Kuluttajat joutuvat maksamaan yksityisyyttä tukevista palveluista. Kanta-asiakkuudesta kieltäytyvät maksavat korkeampia hintoja. Kansalaiset joutuvat näkemään vaivaa tai kieltäytymään suuresta osasta hyvinvointipalveluja välttyäkseen jatkuvilta rekisteröinneiltä. Työntekijät tinkivät tavoitettavuudestaan – jos se ylipäätään on mahdollista – säilyttääkseen edes vähän yksityisyyttään.

Lupaukset ubiyhteiskunnan mukana avautuvasta paratiisista voivat osoittautua matkalipuiksi yksityisyyden lopettajaisiin uudessa Panopticonissa. Teknologiat sinänsä eivät lopeta, eivätkä lähtökohtaisesti edes vaaranna ihmisten yksityisyyttä, mutta ne tarjoavat valvonnalle äärimmäisen tehokkaita välineitä. Yksityisyydestä tekevät lopun teknologioiden käyttöönottajat ja heidän arvovalintansa. Hekään eivät ehkä halua tehdä tällaisia valintoja käytännössä, ainakaan tietoisesti. Sitä ei tosin tarvitakaan – riittää, kun ei tehdä mitään valintaa.

Miksi valvonta sitten nähdään kielteisenä yksityisyyden kannalta? Ubiyhteiskunnan kehittämisessä näkyy uuskieli, jossa asia on ilmaistu myönteisesti: ”ehdotetuilla (työntekijöiden viestinnän valvontaa koskevilla) säännöksillä voidaan arvioida olevan myönteisiä vaikutuksia viestintäverkkojen ja palvelujen käyttäjien yksityisyyden kannalta” (LVM, 2007). Ubiikkiin kulttuuriin kuuluu luonnollisena asiana yksityisyyden kaventuminen – sellaisena se ainakin esitetään.

Lainsäädäntö ja yksityisyys

Mureneva yksityisyydensuoja

Ihmiset lähtevät siitä, että lait tarjoavat heille sellaista yksityisyyttä, kuin he haluavat. He ovat väärässä. Yksityisyys on murentunut varsinkin viime vuosikymmeninä eli juuri aikana, jolloin yksityisyyden suojaa on yritetty turvata nimenomaisesti lakien avulla. Tämä suuntaus on viime vuosina vain voimistunut.

Yksityisyyden suojan nykyaikainen sääntely kytkeytyy kiinteästi henkilötietojen käsittelyn automatisointiin. Julkishallinto alkoi rakentaa suuria atk-järjestelmiä aikana, jolloin ajattelua hallitsivat pelot orwellilaisesta yhteiskunnasta ja pelottelut Itä-Euroopan totalitarismeilla. Monet yksityisyyden sääntelyn argumenteista perustuivat huoleen valvonnan lisääntymisestä.

1970- ja 1980-luvuilla säädettiin monissa Euroopan maissa tietosuojalakeja. Näiden juuret ovat keskitetyn tietojenkäsittelyn ajoilta. EU:n tietosuojadirektiivi ja siihen pohjautuvat kansalliset tietosuojalait, esimerkiksi henkilötietolaki Suomessa, antavat hyvän perustan hallita henkilötietojen keskitettyä käsittelyä ja rekisterinpitoa.

Henkilötietolain keskeinen tavoite on täyttää EU:n tietosuojadirektiivin artiklat, ei yksityisyyden suojan parantaminen tai edes säilyttäminen sinänsä. Viimeistään 2000-luvulla politiikantekijöillekin on selvinnyt, että kyse ei voi olla yksityisyyden suojan parantamisesta. Tarkoituksenmukaista on pyrkiä hallitsemaan teknologisen ja muun kehityksen kielteisiä vaikutuksia yksityisyydelle. Itse asiassa tänään monet turvallisuuteen liittyvät pelot ovat lisänneet vaatimuksia väljentää yksityisyyden suojaa ja sen sääntelyä.

Tietosuojalainsäädännön taustalla on ajattelu, että pyritään tasapainottamaan eri intressejä. On tarve yhtäältä suojata yksityisyyttä henkilötietojen käsittelyssä, toisaalta tarve käyttää tietoja hallinnon ja yksityisen sektorin päätöksentekoon.

Tässä yksityisyyden vastapainoksi asetetaan sellaisia intressejä, kuten hallinnon ja palvelujen tehokkuus, turvallisuus sekä esimerkiksi erilaisten etuuksien ja velvoitteiden oikeudenmukainen kohdentuminen. Näitä on helppo perustella, vaikka ne merkitsisivät kutistuvaa yksityisyyttä. Totta kai moniin niistä sisältyy myös yksityisyyttä tukevia elementtejä.

Henkilötietojen käsittelyn sääntelyllä ei oteta kantaa siihen, minkälaista yksityisyyden tasoa pidetään hyvänä ja hyväksyttävänä. Ei voi

yleisesti sanoa, että sääntely olisi epäonnistunut. Kuitenkin esimerkiksi henkilötietolain velvoitteet tulevat helposti tehottomiksi, kun tietojen keruun, käsittelyn ja käytön tehtävät ja tekijät hajaantuvat tietoverkkoihin ja sulautuvat elämisen perusrakenteisiin. Sen periaatteet eivät tule toimimaan ubiikkiympäristössä.

Henkilötietolaki ja muutkin tietosuojasäädökset antavat periaatteet henkilötietojen käsittelyn laittomuuksien ja väärinkäytösten estämiseksi. Säädöksistä huolimatta on helppo löytää perusteet tietojen käsittelylle, joka puuttuu yksityisyyteen hyvinkin radikaalisti. Kansalaisten viestinnän kattava rekisteröinti, työntekijöiden valvonnan lähes esteetön laajeneminen ja asiakkaiden läpitunkevan profiloinnin yleistyminen mahtuvat helposti lakien raameihin. On vaikea kuvitella, että sääntely pysäyttäisi tai edes merkittävästi hidastaisi organisaatioiden tiedon kasvavien tarpeiden tyydyttämistä.

Lait eivät mukaudu ubiympäristöön

Yksityisyyden suojaamista verkkoympäristössä sääntelyn avulla on pidetty vaikeana, mutta paljon vaikeampaa sen on arvioitu olevan ubiympäristössä. Näkemys on ajankohtaisempi kuin koskaan. Sääntelyn toimimattomuus verkko- ja varsinkin ubiympäristössä tulee esille usealla tavalla. Lait mukautuvat vaikeasti verkottuneen ja rakenteisiin sulautuneen tietojenkäsittelyn vaatimuksiin. Säädöksiä on hankala tulkita ja soveltaa.

Lainsäädäntö on syntynyt ympäristössä, jossa fyysisesti näkyvä rekisterinpitäjä ja rekisteröity olivat yhteydessä keskenään. Sääntelyn kohteena oli näkyvä puuttuminen yksilön elämään. Ubiympäristössä tilanne on aivan toinen. Tulevaisuus on täynnä tietoja käsitteleviä näkymättömiä laitteita ja tunnistimia, joiden olemassaolosta ihminen ei tiedä.

Pirstoutuneessa tietojenkäsittelyn ympäristössä on vaikea löytää vastausta siihen, kuinka tietojen käsittelyn vastuut pitää jakaa. Kenen pitää huolehtia käyttäjien oikeuksista ja käsittelijöiden velvoitteista? Toki näissäkin ympäristöissä on vanhaa tietojenkäsittelyä, keskitettyjä rekistereitä ja rekisterinpitäjiä, mutta niiden merkitys vähenee koko ajan.

Yksityisyyden suojaa koskevien oikeuksien ydin on yksilön oikeus tietää rekistereistä, niiden tietosisällöistä ja käsittelyistä. Samoin oikeus kontrolloida tietojensa ja niiden käsittelyn asianmukaisuutta. Hänellä tulisi olla tiedollinen itsemääräämisoikeus.

Verkkoympäristössä yksilön kyky käyttää lain tarjoamia oikeuksia heikkenee, ubimaailmassa niistä on turha edes puhua. Siellä yksilön on

toivotonta yrittää kontrolloida tietojensa käsittelyä ja välttyä asiattomalta puuttumiselta elämäänsä.

Tietosuojasäädöksillä haetaan yhdenvertaisuutta ja oikeudenmukaisuutta tietojen käsittelyssä ja käytössä. Näiden toteutumista on vaikea arvioida ubiympäristössä, koska itse tietojen keruuta, käyttöä ja siirtoa on vaikea kontrolloida.

Säädöksillä haetaan tasapainoa yksityisyyden ja esimerkiksi valvonnan kesken. Ubiympäristöön on rakennettu kaikkea seuraava ja kirjaava ominaisuus, joka sysää painopistettä valvonnan suuntaan.

Sääntelyn perustana on perinteinen käsitys yksityisyydestä. Ubiikkiympäristössä ollaan kuitenkin siirtymässä perinteisestä rekisterien offline-yksityisyydestä verkkojen online- ja ubimaailman instant-yksityisyyteen. Ubimaailmassa yksityisyys on jotain sellaista, jota nykyisen sääntelyn on vaikea tavoittaa. Instant-yksityisyys toteutuu tai jää toteutumatta ”tässä hetkessä”. Sääntely otetaan tarpeettomana, joskin aika harmittomana riesana, joka on helppo kuitata fraasilla ”tietosuoja täytyy ottaa huomioon”.

Ubimaailman tehoton sääntely

On yleisesti tiedetty, että yksityisyyden sääntelyn vaikutukset ovat heikentyneet ubimaailmassa. On kyseenlaistettu ylipäätään perinteiseen yksityisyyden käsitteeseen perustuvan sääntelyn tarkoituksenmukaisuus siellä. Pääsyy tähän on uusi teknologia, vaikka säädöksiä kirjoitettaessa niitä esitetään teknologian suhteen neutraaleina.

RFID-siruja, biometriikkaa ja muita tunnistimia sekä seuranta- ja jäljityslaitteita otetaan yhä enemmän käyttöön työpaikoilla, oppilaitoksissa, virastoissa ja laitoksissa, liikenteessä ja kodeissa. Sääntely kohdistuu hallinnollisiin käytäntöihin, mikä jättää uuden teknologian käyttötavat helposti sääntelyn katvealueille. Sääntely kokonaisuudessaan kulkee kehittyvän teknologian jäljessä.

Sääntelyn tehottomuus on vakava ongelma ubiympäristössä. Kuitenkin juuri siinä ympäristössä sen tulisi olla aiempaakin toimivampaa, koska käyttäjille näkymättömässä tietojenkäsittelyn ympäristössä heidän mahdollisuutensa turvata muulla tavalla yksityisyyttään ovat heikot.

Tietojen aivan uudenlainen käsittely edellyttää uudenlaista ajattelua myös sääntelyltä. Sen riippumattomuus teknologiasta joudutaan arvioimaan uudelleen. Huomisen yksityisyyden haasteena on teknologioiden hallinta ehkä hyvinkin räätälöityjen säädösten avulla.

Jokapäiväisissä laitteissa ja hyödykkeissä olevat tietokoneet ja kaikkialla olevan tunnistamisen ja kontrollin lähes rajaton mahdollisuus edellyttävät säädösten ja normien uudelleen arviointia. ”Älykkyys” arkisessa ympäristössämme kasvaa nopeasti, tämän tulisi näkyä myös sitä koskevassa sääntelyssä. Siksi on yllättävää ja huolestuttavaakin, että esimerkiksi EU:n komissio ei pidä tarpeellisena tietosuojasäädösten tarkistamista.

On epäilty mahdollisuutta siirtää sääntelyä alueille, missä ”uuteen yksityisyyteen” sisältyvät ihmisen ruumis, ruumiin toiminnot ja liikkeet ja ihmisen fysiologiset reaktiot. Vastausta vailla on myös identiteetin hallinta, kuka omistaa yksilön identiteetin? Ubimaailman arkipäivää on identiteettien sieppailu ”lennosta”. Tietosuojasäädökset eivät tunne kyseistä varkautta rikoksena. Tällaisten asioiden yksityisyyden suoja on jotain muuta kuin rekisterissä olevien henkilötietojen yksityisyyden suoja.

Satelliitit seuraavat jokaista, jolla on matkapuhelin tai joka käyttää tietoverkkoa. Vaikka olisi tiukatkin tietosuojalait, avaruudesta tulevalta valvonnalta on vaikea suojautua kenenkään matkapuhelimen tai verkon käyttäjän. Tällainen valvonta on paljolti kansallisten säädösten ulottumattomissa. Edes kansainväliset säädökset, esimerkiksi EU:n tietosuojadirektiivi, eivät ulotu tällaiseen puuttumiseen yksityisyyteen.

Uudelleenajattelua lainsäädäntöön

Yhteiskuntia ja talouksia kohtaavat globaalit uhat. Nämä vaativat yhteistoimintaa, valvontaa ja puuttumista yksityisyyteen globaalilla tasolla. Ubiikissa maailmassa yksityisyyteen puuttumisen käytännöt ovat hyvin paikallisia, siellä yksityisyyden suojaamisen ratkaisut tulisi räätälöidä yksilökohtaisiksi. Tässä ratkaisujen yhteismitattomuudessa yksityisyys yleensä väistyy.

On väitetty, että vallitseva tietosuojan malli sääntelyineen ja sitä toteuttavine byrokratioineen ei enää toimi ja että sääntely ylipäätään edustaa virheellistä byrokraattista tarkastelutapaa (Marx, 1985). Se luo epäonnistumisia käytännössä. Yksityisyyden suoja rapautuu kovaa vauhtia ja toteutunut yksityisyys erkanee kaiken aikaa lain mukaisesta yksityisyyden suojasta. Toki lakien byrokraattiset velvoitteet on helppo täyttää tai ohittaa.

On kysytty, onko yksityisyys kuollut (Froomkin, 2000). Jos yksityisyys kerran on kuollut, tarvitaanko sen sääntelyä? Sääntelyn uudel-

leenajattelu on tarpeen ennen kaikkea sen selvittämiseksi, mikä on yhä elävää, mikä jo kuollutta yksityisyyttä ja sen sääntelyä. Nykyisellään säädösten kyvyttömyys pikemmin mahdollistaa ja laillistaa yksityisyyden murentamisen.

Yritykset hillitä valvontayhteiskunnan etenemistä uusilla säädöksillä arvatenkin voimistuvat, mutta kehityksen suuntaa nekään eivät käännä. Jos uskotaan, että tietosuojasäädökset pelkällä olemassaolollaan varmistavat yksityisyyden jatkossakin, on syytä pelätä yksityisyyden pahimpien uhkakuvien toteutumista.

Ubiteknologioita pidetään tietoyhteiskunnan innostuksessa edistyksen merkkeinä. Ellei tunnusteta niiden varjopuolta, eikä ymmärretä sääntelyn rajattua roolia, ubiyhteiskunnan seuraukset yksityisyydelle voivat olla tuhoisat.

Kirjallisuutta

Bentham, Jeremy, The Panopticon Writings. Miran Bozovl, ed. London, Verso, 1995

Brin, David, The Transparent Society; Will Technology Force Us to Choose Between Privacy and Freedom? Reading, MA, Addison-Wesley, 1998

Clarke, Roger, Information Technology and Dataveillance. Communications of the ACM, 31(5), 1988

Clarke, Roger, The Digital Persona and its Application to Data Surveillance. The Information Society, 10, 1994

Clarke, Roger, Computer Matching and Digital Identity.
http://www.anu.edu.au/people/Roger.Clarke/DV/CFP93.html

Clarke, Roger, Trails in the Sand.
http://www.anu.edu.au/people/Roger.Clarke/DV/Trails.html

Dwyer, Catherine – Hiltz, Starr – Passerini, Katia, Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace. Proceedings of the Thirteenth American Conference on Information Systems, Colorado, 2007

The Economist, The End of Privacy. May, 1999

Ehdotus sähköisen viestinnän tietosuojalain muuttamiseksi, Liikenne- ja viestintäministeriön julkaisuja 29/2007

Foucault, Michel, Tarkkailla ja rangaista. Otava, 1980

Froomkin, Michael, The Death of Privacy? Standard Law Review, 52, 1461-1543, 2000

Garfinkel, Simon, Database Nation, The Death of Privacy in the 21st Century. Beijing, O'Reilly, Cambridge, 2000

Gotlieb, Calvin, Privacy; A Concept Whose Time Has Come and Gone. In: Lyon&Zureik, 1996

Gross, Ralph – Acquisti, Alessandro, Information Revelation and Privacy in Online Social Networks (The Facebook Case). ACM Workshop on Privacy in the Electronic Society, 2005

Heinonen, Risto, Digitaalinen minä. Edita, 2001

Heinonen, Risto, Digitaaliset jäljet – identiteettisuoja ja tunnistaminen tietoverkoissa. Hyvinvointikatsaus 3/2001, Tilastokeskus, 2001

Heinonen, Risto – Hannula, Ilari, Valvonta tietoyhteiskunnassa. Edita, 1999

Julkishallinnon sähköisen asioinnin rakenneosat. VM, 30.5.2007

Koskela, Hille, "Cam Era" – the Contemporary Urban Panopticon. Surveillance & Society, 1(3), 2003

Langheinrich, Marc, Personal Privacy in Ubiquitous Computing. Research Seminar, Lancaster University, UK, November 14, 2005

Langheinrich, Marc, Privacy Invasions in Ubiquitous Computing. http://quir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/uc2002-pws.pdf

Lyon, David, Zureik, Elia (eds.), Computers, Surveillance and Privacy. University of Minnesota Press, London, 1996

Marx, Gary T, The Surveillance Society; the Threat of 1984-style Techniques. The Futurist, June, 1985

Orwell, George, Vuonna 1984. WSOY, 1967

A Report on the Surveillance Society.Ed. by D. Murakami. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

Ström, Pär, Med storebror i baksätet – digital övervakning av dina bilfärder. Den nya välfärden, 2006

Ström, Pär, Med storebror i byxfickan, från snokande kläder till människokartor – integritetsrisker med RFID-chips. Den nya välfärden, 2007

Uusi arjen tietoyhteiskunta, taustaselvitys liikenne- ja viestintäministeriölle. 6.3.2006

Weber, Max, The Theory of Social and Economic Organizations. London, W. Hodge, 1947

Westin, Alan, Privacy and Freedom. Atheneum, New York, 1967

Whitaker, Reg, The End of Privacy. The New Press, New York, 1999

WIRED, Sun on Privacy; “Get Over It”. 1999

Wood, David, Foucault and Panopticism Revisited. Surveillance & Society, 1(3), 2003

Wright, Tom, A Case of Mistaken Identity. An International Study of Identity Cards, 1995

Olemme matkalla ubiikkiyhteiskuntaan eli “arjen tietoyhteiskuntaan”. Sen kaikkialle ulottuva ja ympäristöön sulautuva tiedonkeruu koskettavat jokaista kansalaista.

Ubiikkiteknologia tulee muuttamaan arjen rajoja ja oikeudellisia käsityksiä. Muutospaineet kohdistuvat erityisesti kansalaisen yksityisyyteen ja tietosuojaan, mutta ne ravistelevat myös laajemmin lainsäädäntöä, oikeudellisia käsitteitä ja yhteiskunnan toimintaperiaatteita. Tietoteknologinen kehitys on tuomassa mukanaan uuden yhteiskunnallisen murrosvaiheen.

Ubiikki tulee jokaiseen kotiin. Millainen maailma sitten tulee ulottumaan jokaisen arkeen? Miten ubiikkimaailman oikeudet ja pelisäännöt muodostuvat? Mitä vaikutuksia muutoksilla on kansalaisten oikeuksiin?

Julkaisuun on koottu puheenvuoroja ubiikkiyhteiskunnasta ja digitaaliseen tietoon liittyvistä oikeudellisista kysymyksistä.

EDUSKUNNAN KIRJASTON TUTKIMUKSIA JA SELVITYKSIÄ 10