

# Turvallisten sisältöjen valikointi ja arviointi

Tietoa verkkosisältöjen teknisistä suodatin- ja estojärjestelmistä

Opetusministeriön työryhmämuistioita ja selvityksiä 2006:8

# Turvallisten sisältöjen valikointi ja arviointi

Tietoa verkkosisältöjen teknisistä suodatin- ja estojärjestelmistä

Opetusministeriön työryhmämuistioita ja selvityksiä 2006:8



OPETUSMINISTERIÖ

*Undervisningsministeriet*

MINISTRY OF EDUCATION

*Ministère de l'Éducation*

Opetusministeriö / Undervisningsministeriet  
Kulttuuri-, liikunta- ja nuorisopolitiikan osasto /  
Kultur-, idrotts- och ungdomspolitiska avdelningen  
PL / PB 29  
00023 Valtioneuvosto / Statsrådet  
<http://www.minedu.fi/julkaisut/index.html>

Yliopistopaino / Universitetstryckeriet, 2006

ISBN 952-485-100-8 (PDF)

ISSN 1458-8102

Opetusministeriön työryhmämuistioita ja selvityksiä/  
Undervisningsministeriets arbetsgruppspromemorior och utredningar 2006:8

## Kuvailulehti

Julkaisija  
Opetusministeriö

Julkaisun päivämäärä  
28.2.2006

<p><b>Tekijät</b> (toimielimestä: toimielimen nimi, puheenjohtaja, sihteeri)</p> <p><b>Turvallisten sisältöjen valikointi ja arviointi -tekniset järjestelmät työryhmä</b> Asiantuntija: Nixu Oy</p>	<p><b>Julkaisun laji</b> Opetusministeriön työryhmämuistioita ja selvityksiä -verkkojulkaisu</p>	
	<p><b>Toimeksiantaja</b> Opetusministeriö</p>	
	<p><b>Toimielimen asettamispv</b> 16.12.2005</p>	<p><b>Dnro</b> 74/040/2005</p>
<p><b>Julkaisun nimi</b> (myös ruotsinkielinen) <b>Turvallisten sisältöjen valikointi ja arviointi</b></p>		
<p><b>Julkaisun osat</b> Muistio + liite</p>		
<p><b>Tiivistelmä</b></p> <p>Internetissä on sekä laittomia että laillisia mediasisältöjä, jotka molemmat voivat olla haitallisia lasten ja nuorten kasvulle ja kehitykselle. Suodatin- ja estojärjestelmät tarjoavat tekniset välineet estää alaikäisiä joutumasta kohtaamaan paitsi laitonta aineistoa myös muuta kehitystasolleen haitallista sisältöä.</p> <p>Tämä selvitys on tuotettu osana opetusministeriön Lapset ja Media -ohjelmaa. Selvityksen tarkoituksena on tuottaa kuntien, koulujen, kirjastojen ja kotitalouksien tarpeisiin tietoa lapsille ja nuorille haitallisia sisältöjä koskevista suodatin- ja estojärjestelmistä. Selvityksen tarkoituksena ei ole suositella eikä torjua suodatin- ja estojärjestelmien käyttöä. Tarkoituksena ei ole myöskään suositella jonkin tietyn mediasisällön suodattamista.</p> <p>Suomessa on tarjolla sekä kotimaisia että ulkomaisia suodatin- ja estojärjestelmiä, -palveluja ja -tuotteita. Pääosa nykyisistä järjestelmistä perustuu erilaisiin ylläpitoa edellyttäviin listoihin tai tietokantoihin, joiden avulla tietoverkon käyttöä pyritään rajoittamaan. Rajoitus voidaan tehdä rajoittamalla pääsy vain kiellettyihin aineistoihin tai kieltämällä pääsy kaikkeen paitsi sallittuun aineistoon. Nykyään suurin osa menetelmistä perustuu pääsyn rajoittamiseen osaan Internetistä.</p> <p>Pienen yhteisön ja kotitalouksien tarpeet voidaan tyydyttää yhden ohjelmiston asentamisella tai suodatinlaitteen kytkemisellä verkkoon ja verkon liikenteen ohjaamisella laitteen läpi.</p> <p>Suuremmat suodatinjärjestelmät voidaan koota monista eri verkkolaitteista ja eri järjestelmien yhdistelmästä.</p> <p>Suurempien suodatinjärjestelmien rakentamisen ja ylläpidon kustannukset voivat nousta korkeiksi, jolloin käytännössä ainoaksi mahdollisuudeksi voi jäädä suodatuspalvelun ostaminen palveluntarjoajalta. Tällöin on syytä kiinnittää huomiota erityisesti palvelun sisältöön ja palvelun laadun takaavaan palvelutasosopimukseen.</p> <p>Jotta järjestelmän toimivuus olisi moitteetonta, tulee järjestelmän hallinnointiin kiinnittää huomiota. Poliitikkojen, käytäntöjen, prosessikuvausten ja ohjeiden avulla pystytään määrittelemään se, mitä varsinaisen systeemin ylläpitohenkilöstön tulee tehdä ja missä rajoissa.</p> <p>Suodatusjärjestelmät eivät kaupallisista syistä pysty koskaan olemaan täysin läpinäkyviä. Läpinäkyvyyttä voidaan parantaa julkistamalla muutosmenetelmät ja tarjoamalla tekniset keinot ohittaa virheellinen suodatettava kohde kohtuullisessa ajassa.</p> <p>Selvitykseen on järjestelmien käyttöönottoa suunnittelevien arvioinnin helpottamiseksi liitetty muistilista asiassa huomioon otettavista kysymyksistä.</p>		
<p><b>Avainsanat</b></p>		
<p><b>Muut tiedot</b></p>		
<p><b>Sarjan nimi ja numero</b> Opetusministeriön työryhmämuistioita ja selvityksiä 2006:8</p>	<p><b>ISSN</b> 1458-8102</p>	<p><b>ISBN</b> 952-485-100-8 (PDF)</p>
<p><b>Kokonaissivumäärä</b> 30</p>	<p><b>Kieli</b> suomi</p>	<p><b>Hinta</b> - <b>Luottamuksellisuus</b> julkinen</p>
<p><b>Jakaja</b></p>	<p><b>Kustantaja</b> Opetusministeriö</p>	

# Saatteeksi lukijalle

Tämä selvitys on tuotettu osana opetusministeriön Lapset ja Media -ohjelmaa<sup>1</sup>.

Lapset ja Media -ohjelma pohjautuu pääministeri Matti Vanhasen hallituksen ohjelmaan, jonka mukaan hallitus käynnistää toimintaohjelman lapsiin ja nuoriin kohdistuvan media-väkivallan haittojen vähentämiseksi. Lukuisissa tutkimuksissa on osoitettu, että mediaväkivalta vaikuttaa ihmisiin ja erityisesti lapsiin ja nuoriin. Vaikutukset ilmenevät jäljittelynä, aggressiivisuuden lisääntymisenä, pelkoina, virheellisinä käsityksinä ja turtumisena. Lapset ottavat vaikutteet herkästi mallioppimisen kautta.

Tekninen kehitys on johtanut muun muassa viestintävälineiden sisältöjen määrän moninkertaistumiseen, käyttötapojen monipuolistumiseen ja sisältöihin pääsyn helpottumiseen. Uudessa tilanteessa pelkästään perinteiset tarkastamiseen, ikärajaluoituksiin ja aikarajoituksiin perustuvat järjestelmät eivät voi kattaa kaikkia sisältöjä. Mediakasvatuksesta tulee yhä tärkeämpi tekijä lapsille turvallisemman mediaympäristön luomisessa.

Mediakasvatusta voidaan toteuttaa kodeissa, kouluissa, kirjastoissa ja myös muiden eri tahojen toimesta. Valistuksen ja mediakasvatuksen lisäksi pienet lapset tarvitsevat aikuisen läsnäoloa ja tukea median käytössä sekä aika- ja sisältörajoituksia lapsen kehitystasoon mukaisesti. Aikuisten tehtävänä on huolehtia, ettei lapsi joudu kosketuksiin kehitystasolleen sopimattomien sisältöjen kanssa.

Suodatin- ja estojärjestelmät tarjoavat yhden välineen estää alaikäisiä joutumasta kohtaamaan haitallista aineistoa. Opetusministeriö asetti 16.12.2005 työryhmän, jonka tehtävänä on ohjata projektia, joka tuottaa kuntien, koulujen, kirjastojen ja kotitalouksien tarpeisiin tietoa lapsille ja nuorille haitallisia sisältöjä koskevien suodatin- ja estojärjestelmien teknisistä ominaisuuksista ja muista käyttöönnotossa huomioitavista asioista.

Projektin pohjaksi opetusministeriö tilasi asiantuntijaselvityksen Nixu Oy:ltä, joka on tietoturvakonsultointiin erikoistunut yritys. Asiantuntijana toimi tietoturvakonsultti Jari Hirvonen.

<sup>1</sup> <http://www.minedu.fi/opm/kulttuuri/ohjelmatyo/mediavakivalta.html>

Selvityksestä käy ilmi, että Suomessa on tarjolla sekä kotimaisia että ulkomaisia suodatin- ja estojärjestelmiä, -palveluja ja -tuotteita. Niitä on myös melko laajasti otettu käyttöön mm. kunnissa ja kouluissa. Järjestelmistä ja palveluista on olemassa alustavia käyttökokeimuksia, joita tässä selvityksessä ei vielä ole koottu. Kokemuksia on syytä tarkastella niiden karttuessa. Esimerkkinä tuodaan esille Espoossa tehdyt ratkaisut tietoliikenteen rakentamisesta internetin sosiaalisiin pelisääntöihin.

Joissakin tietoverkkopalvelujen julkisissa käyttöympäristöissä, kuten monissa kirjastoissa, on arvioitu, että ongelmallisten sisältöjen saatavuuteen on puututtava muilla keinoilla kuin suodatin- ja estojärjestelmillä. Perusteena tälle on ollut mm. se, että esim. kirjastoissa lapset ovat turvallisessa ympäristössä, jossa aikuinen on läsnä. Tärkeintä onkin, että erilaisin keinoin vaikutetaan turvallisen mediaympäristön kehittämiseen.

Tämän selvityksen tarkoituksena ei ole suositella eikä torjua suodatin- ja estojärjestelmien käyttöä. Tarkoituksena ei ole myöskään suositella jonkin tietyn mediasisällön suodattamista. Selvityksen tarkoituksena on antaa järjestelmien käyttöönottoa harkitseville ja muille asiasta kiinnostuneille tietoa niiden toiminnoista ja rajoitteista. Järjestelmien käyttöönottoa suunnitteleville selvitykseen on arvioinnin helpottamiseksi liitetty muistilista asiassa huomiioon otettavista kysymyksistä.

# Sisältö

<b>Johdanto</b>	<b>7</b>
<b>1 Yleistä suodatin- ja estojärjestelmistä</b>	<b>9</b>
<b>2 Hallinnolliset haasteet</b>	<b>11</b>
2.1 Suodatuksen läpinäkyvyys	11
2.2 Suodatuspolitiikka ja -päätökset	12
2.3 Tietoisuuden lisääminen	12
2.4 Viranomaismääräykset ja –suositukset	12
2.5 Suodatuksessa huomioon otettavasta lainsäädännöstä	13
<i>Sananvapaus ja rikoslain piirissä oleva aineisto</i>	13
<i>Sähköisen viestinnän tietosuoja ja henkilötietolaki</i>	14
<i>Käytettävien aineistojen hankinta ja valinta</i>	15
<b>3 Tekniset haasteet</b>	<b>16</b>
3.1 Suodatuksen kattavuus	16
3.2 Suodatuksen yhteneväisyys	18
3.3 Virheet suodatuksessa	18
3.4 Suodatuksen ylläpito ja päivitys	18
3.5 Suodatuksen luokat	19
<b>4 Tekniset vaatimukset suodatukselle</b>	<b>20</b>
<b>5 Nykyiset tekniset ratkaisut</b>	<b>21</b>
5.1 Toimintaperiaate	21
<i>Listoihin perustuvat järjestelmät</i>	21
<i>Luokitteluun perustuvat järjestelmät</i>	21
<i>Tekoälyyn ja säännöstöihin perustuvat järjestelmät</i>	22
5.2 Toteutustapa	22
<i>Hajautetut järjestelmät</i>	22
<i>Keskitetyt järjestelmät</i>	23
<i>Suodatuspalvelut</i>	24
5.3 Ilmaiset järjestelmät	24
5.4 Espoo esimerkkinä: Tietoliikenteen rakentamisesta Internetin sosiaalisiin pelisääntöihin	24
<b>6 Tulevaisuuden ratkaisuja</b>	<b>26</b>
6.1 Automaattinen sisällönhallinta	26
6.2 Keskitetyt sisällönhallintajärjestelmät	26
<b>7 Hankinnassa ja käyttöönotossa huomioon otettavia näkökohtia</b>	<b>27</b>
<b>Liite: Suodatinjärjestelmien hankinnan muistilista</b>	<b>28</b>

# 1 Johdanto

Internetissä tarjolla olevien ongelmallisten sisältöjen saannin estämiseksi tai rajoittamiseksi tarkoitettujen järjestelmien, palvelujen ja tuotteiden toiminnat sivuavat monia periaatteellisesti tärkeitä kysymyksiä. Näitä ovat muun muassa vapaaseen tiedonvälitykseen ja sananvapauteen sisältyvät oikeudet vastaanottaa ja välittää tietoja kenenkään tätä ennakolta estämättä ja aikuisten velvollisuudet huolehtia lapsille turvallisen mediaympäristön luomisesta.

Suomessa on perinteisesti kunnioitettu sanan- ja ilmaisuvapautta. Varsinkin viime aikoina aineistojen sensuroimisen mahdollisuus on kyseenalaistettu. Teknologinen kehitys viimeisen kymmenen vuoden aikana on kuitenkin johtanut tilanteeseen, jossa kaikilla on tietoverkkojen välityksellä mahdollisuus saada nähtävillään aineistoja, joihin verrattuna esimerkiksi aikanaan sensuroinnin kohteeksi joutuneet ”Kravun kääntöpiiri” ja ”Juhannustanssit” olisivat varsin hyväksyttäviä. Ennen sensuroinnin kohteesta nousi kohu. Nykyään kohu nousisi itse sensuroinnista.

Perustuslain 12 §:ssä turvatus sananvapauden, johon sisältyvät ilmaisunvapaus ja tiedonsaannin vapaus, kunnioittaminen ei tarkoita sitä, että Suomen lainsäädäntöön ei voisi sisältyä säännöksiä, joilla rajoitettaisiin Internetissä olevia aineistoja tai niiden levittämistä. Erityisesti perustuslain mukaan voidaan lailla säätää kuvaohjelmia koskevia lasten suojelemiseksi välttämättömiä rajoituksia.

Perusoikeussäännöksistä huolimatta tietyille kriminalisoinneille on katsottu olevan hyväksyttävät perusteet. Rikoslain 17 luvun 19 §:ssä säädetään sukupuolisiveellisyttä loukkaavan lasta esittävän kuvan hallussapidosta. Lapsipornon hallussapito on kiellettyä siitä riippumatta, onko esimerkiksi valokuva tai video tallennettu Internetiin yhteydessä olevalle tietokoneelle tai pidetäänkö kuvaa tai videota hallussa pelkästään sen fyysisenä kappaleena. Myös rikoslain 17 luvun 18 ja 18 a §:n säännökset sukupuolisiveellisyttä loukkaavan kuvan levittämisestä soveltuvat niiden levitystavasta riippumatta. Teknologianeutraalisti arvioidaan myös tilanteet, joissa rikoslain 17 luvun 18 b §:n mukaisesti kuvaohjelmia esitetään tai levitetään laittomasti alaikäiselle.



Mahdollisesta Internet-operaattorien tekemistä lapsipornon estotoimista on erotettava omaksi alueekseen Internet-viestinnän vastaanottajatasolla tapahtuva suodattaminen. Esimerkiksi kuntien kirjastoilla ja kouluilla on niitä koskevan lainsäädännön, viranomaismääräysten ja -ohjeistuksen rajoissa vapaus määrittellä ne lasten ja nuorten kehitykselle sopivat aineistot, joita käyttöönsä hankkivat. Tässäkään ei tehdä eroa Internetissä saatavilla olevan ja fyysisessä muodossa hankittavan aineiston välillä. Kuntien kirjastot ja koulut voivat päättää, mitä lehtiä tai oppimateriaalia ne käyttöönsä hankkivat. Ymmärrettävistä syistä pornolehdet ja väkivaltakuvauksia sisältävät kirjat on jätetty hankkimatta.

Kotona Internetin käytön rajojen asettaminen on lasten vanhempien vastuulla. Tätä voidaan tukea lisäämällä vanhempien tietämystä ja teknisiä valmiuksia rajoitusten tekemiseen. Yksinkertaisimmillaan vanhemmat voivat rajoittaa lasten Internetin käyttöä luomalla käyttöjärjestelmällä lapsille rajattuja käyttöoikeuksia. Tällöin vain vanhemmilla on oikeus asentaa ohjelmia (esim. vertaisverkko-ohjelmia) ja muuttaa käyttöjärjestelmän asetuksia.<sup>2</sup>

Suodatus- ja estomenetelmien suunnittelun ja asennuksen ei tule perustua pelkästään päätökseen, että Internetin käyttöä pitää rajoittaa. On myös tarkasteltava sitä, missä laajuudessa Internetin käyttöä halutaan rajoittaa, keneltä käyttöä rajoitetaan, millä perusteilla rajoitukset tehdään, mitkä ovat toimenpiteet väriin rajoitusten korjaamiseksi ja miten rajoitusten noudattamista valvotaan. Päätöksiä tarvitaan myös siitä, miten pitkälle rajoitukset tulee ulottaa. Tällaisia perusteltuja ratkaisuja ovat erilaiset kansalaisjärjestöt vaatineet hienostuneiden – erityisesti automaattisten – systeemien sijaan.

Internetin käyttöä voidaan varsin paljon rajoittaa teknisillä menetelmillä. Mikäli laajamittaiseen suodatustoimintaan siirryttäisiin, se vaatisi pitkälle vietyjä järjestelmiä, joilla pystytään sekä estämään järjestelmän kiertäminen että paljastamaan kiertäjät. Tällaisten järjestelmien rakentaminen ja ylläpito tulee kalliiksi.

Suodatinjärjestelmät eivät kaupallisista syistä pysty koskaan olemaan täysin läpinäkyviä. Läpinäkyvyyttä voidaan parantaa julkistamalla muutosmenetelmät ja tarjoamalla tekniset keinot ohittaa virheellinen suodatettava kohde kohtuullisessa ajassa.

Jotta järjestelmän toimivuus olisi moitteetonta, tulee myös järjestelmän hallinnointiin kiinnittää huomiota. Poliitikkojen, käytäntöjen, prosessikuvausten ja ohjeiden avulla pystytään määrittelemään se, mitä varsinaisen systeemin ylläpitohenkilöstön tulee tehdä ja missä rajoissa.

Erilaisia ja eri periaatteilla toimivia kaupallisia järjestelmiä on olemassa. Riittävän kattavuuden takaavia järjestelmiä ei kuitenkaan ole paljon markkinoilla, ja usein suodatinjärjestelmä voi koostua useasta eri systeemistä tai järjestelmän osista.

Seuraavissa luvuissa esitellään erilaisia teknisiä keinoja rajoittaa Internetin käyttöä. Samoin pyritään löytämään hyviä toimintatapoja näiden systeemien hallintaan ja ylläpitämiseen. Tavoitteena on valistaa päättäjiä ja toteuttajia teknisistä suodatuskeinoista, niiden puutteista sekä niihin liittyvistä hallinnollisista toimista. Tarkoituksena ei ole suositella suodattamista eikä torjua sitä. Tarkoituksena ei ole myöskään suositella jonkin tietyn mediasäällön suodattamista.

---

<sup>2</sup> Useimmat nykyään käytettävät käyttöjärjestelmät ovat monen käyttäjän käyttöjärjestelmiä.  
<http://www.tietoturvaopas.fi/fi/index.html>

# 1 Yleistä suodatin- ja estojärjestelmistä

Pääosa nykyisistä järjestelmistä perustuu erilaisiin ylläpitoa edellyttäviin listoihin tai tietokantoihin, joiden avulla tietoverkon käyttöä pyritään rajoittamaan. Rajoitus voidaan tehdä rajoittamalla pääsy vain kiellettyihin aineistoihin<sup>3</sup> tai kieltämällä pääsy kaikkeen paitsi sallittuun aineistoon<sup>4</sup>. Nykyään suurin osa menetelmistä perustuu pääsyn rajoittamiseen osaan Internetistä. Pääsyä voidaan rajoittaa joko suodattamalla, jolloin pääsyä rajoitetaan estämällä pääsy osaan materiaalista, tai estämällä, jolloin pääsyn rajoittamisen voidaan katsoa olevan kokonaisvaltaisempaa esimerkiksi torjuttaessa liikenne jonkun tietoliikenneprotokollan osalta täysin.

- *Tyypillisesti tällainen järjestelmä pystyy kontrolloimaan liikennettä muutamalla samankaltaisella tietoliikenneprotokollalla kuten webliekenteen HTTP- ja HTTPS-protokollilla.*

Suodatuspalvelu voidaan toteuttaa yksinkertaisimmillaan tilaamalla suodatuspalvelu Internet-palveluntarjoajalta. Pienen yhteisön tarpeet voidaan tyydyttää yhden ohjelmiston asentamisella tai suodatinlaitteen kytkemisellä verkkoon ja verkon liikenteen ohjaamisella laitteen läpi. Suuremmat suodatinjärjestelmät voidaan koota monista eri verkkolaitteista ja eri järjestelmien yhdistelmistä.

Järjestelmä voidaan asentaa palvelimiin, jotka ovat jatkuvasti tietoverkkoihin kytkettyinä ja joiden kautta yhden tai useamman käyttäjän pöytätietokoneen liikenne ohjataan. Järjestelmä voi olla myös valmiiksi asennettuna tietoliikennelaitteeseen, jonka ainoa tarkoitus on toteuttaa suodatuspalveluja.

Järjestelmään voi lisäksi liittyä kuormantasauslaitteita, palomuureja, reitittämiä, kytkimiä tai muita tietoliikennelaitteita, joiden tarkoitus on täydentää suodatuspalveluja tai varmentaa palvelun saatavuus vikatilanteissa tai turvata järjestelmää tai vaikka vain kytkeä järjestelmä osaksi suurempaa verkkoa tai -palvelua.

---

<sup>3</sup> Suodatusmenetelmän periaatteena on päästää läpi kaikki muu paitsi määritelty kielletty aineisto. Tämä tunnetaan ns. Black list -menettelynä.

<sup>4</sup> Suodatusmenetelmän periaatteena on estää kaikki muu liikenne paitsi erikseen määritelty sallittu aineisto. Tämä tunnetaan ns. White list -menettelynä. White list -menettely voi olla käyttökelpoinen lisä kodeissa ja päiväkodeissa tapahtuvan pienten lasten Internetin käytön rajoittamisessa.

Järjestelmään kuuluvia lisätoimintoja voivat olla liikenteeseen liittyvän tilastotiedon, suodatus-tapahtumien kerääminen, suodatinjärjestelmään kirjautumisyrityksen ja muun tarvittavan tiedon kerääminen.

Lisäksi järjestelmä voi päästää käyttäjän käyttämään verkkopalvelua hakemalla käyttäjätunnuksen ja salasanan toiselta koneelta, tai käyttäjän tunnistaminen voi olla osa järjestelmää.

Järjestelmän toiminnallisuutta voidaan tarkkailla erillisellä valvontaohjelmistolla, joka voi olla osa järjestelmän toiminnallisuutta, tai erillisellä valvontajärjestelmällä, joka näyttää järjestelmän tilan osana muuta verkonvalvontaa. Valvontaohjelmisto voidaan lisäksi asentaa hälyttämään, mikäli järjestelmä vikaantuu tai siihen kohdistuu normaalia suurempi tai pienempi määrä liikennettä.

Suodatuspalvelukin voidaan määrätä suodattamaan vain tiettyä osaa siihen valmiiksi määritellyistä kohteista. Niihin voidaan myös itse lisätä tarpeelliseksi katsottuja kohteita, ja osiin tuotteista voidaan tehdä poikkeuksia, joiden avulla taataan pääsy listoilla virheellisesti olevaan materiaaliin tai voidaan poistaa virheelliset kohteet niistä.

Myös Internetin sisältö lisääntyy, poistuu ja vaihtuu. Sitä kopioidaan, muutetaan ja siirretään paikasta toiseen käyttämällä useita eri protokollia ja tekniikoita. Tiedostoja pakataan, puretaan ja nimetään uudelleen. Myös haitalliseen materiaaliin ja sen levittämiseen pätevät nämä lait, mutta ehkä eri kontekstissa. Suodatinjärjestelmä onkin valmistuttuaan vanhentunut, mikäli sitä ei kyetä päivittämään säännöllisesti.

Teknisillä menetelmillä, joita esimerkiksi operaattorit kansallista suodattamista tehdessään käyttävät, saavutetaan yleensä rajoitettu suodattaminen, joka on teknisesti edistyneen varsin helppo kiertää. Yleensä kiertämismenetelmät myös pian paljastetaan julkisuudessa sillä tarkkuudella, että tavallisetkin käyttäjät pystyvät melko helposti ja vaivattomasti kiertämään hienostuneitakin järjestelmiä. Järjestelmien kierto on nykyään kohtuullisen helppoa myös tietoliikenneprotokollien lukumäärän sekä erilaisten salaus-, pakkaus- ja muiden keinojen käytön vuoksi.

## 2 Hallinnolliset haasteet

### 2.1 Suodatuksen läpinäkyvyys

Suodatinohjelmat ovat yleensä kaupallisia tuotteita johtuen niiden jatkuvasta päivitystarpeesta. Yhtiöillä on luonnollisesti oikeus pitää liikesalaisuutenaan kohteet, joiden paljastamiseen on voitu käyttää merkittävästi resursseja ja jotka itse asiassa –kehitetyn ohjelmiston sijasta – muodostavat yrityksen tuotteen. Vaatimus siitä, että listat olisivat julkisia<sup>5</sup>, ei liene realistinen<sup>6</sup>.

Tästä syystä se, mitä suodatetaan, ei yleensä ole käyttäjän tiedossa. Tällöin käyttäjä ei voi etukäteen tietää, mitä kaikkea suodatetaan ja onko hänellä pääsy tähän aineistoon.

Läpinäkyvyyttä voidaan kuitenkin parantaa ilmoituksellisin keinoin. Tällöin käyttäjälle ilmoitetaan selkeästi, että nimenomaan haettuun materiaaliin pääsy on kyseisellä laitteella kielletty. Tosin tällä menettelyllä käyttäjä ei voi olla varma, onko kohde oikein määritelty, mikäli hän ei sitä itse pääse tarkistamaan. Käyttäjälle voidaan antaa mahdollisuus pyytää materiaaliin pääsy, jos suodatinohjelma toimii tämän kohteen kohdalla väärin.

Sisällön vapauttamisen periaatteet, toimintatavat ja vasteajat tulisi ilmoittaa julkisesti. Mikäli mahdollista, käyttäjän tulisi lisäksi saada kohtuullisessa ajassa tieto siitä, avattiinko pääsy kohteeseen vai ei. Päätökset ja niihin johtaneet syyt tulisi arkistoida.

Tämänkaltaiset suositukset toimintatavoista voivat asettaa toimintatavoille, resursseille ja järjestelmille sellaisia vaatimuksia, että pienemmille yhteisöille voi koitua järjestelmän ylläpidosta merkittäviä rasitteita.

---

<sup>5</sup> <http://www.effi.org/julkaisut/tiedotteet/lehdistotiedote-2005-02-04.html>; ensimmäinen kriteeri

<sup>6</sup> [http://www.saunalahhti.fi/~hohakkar/fabula/2005\\_02\\_01\\_archive.html#110900067052899106](http://www.saunalahhti.fi/~hohakkar/fabula/2005_02_01_archive.html#110900067052899106)

## 2.2 Suodatuspolitiikka ja -päätökset

Organisaation eri osissa tehtävät suodatinohjelmien toteutukset tulisi yhtenäistää politiikoin ja ohjein sekä määrittää käytännöt, joilla päätökset suodatinohjelmien käytöstä, kattavuudesta ja valvontatoimista tehdään ylläpito-organisaatiossa.

- *Suodatuspolitiikassa voidaan määrittää mitä suodatetaan, sekä kuka vastaa suodatuksen toteuttamisesta, sen hallinnasta ja suodatukseen liittyvistä päätöksistä.*

Jotta järjestelmän toteutus ja ylläpito voitaisiin toteuttaa tarkoituksenmukaisesti ja suodatinjärjestelmälle asetettujen odotusten mukaisesti, tulisi järjestelmän käyttö, ylläpito ja hallinnointi ohjeistaa riittäväällä tarkkuudella.

Lisäksi käyttäjät tulisi sitouttaa tietojärjestelmän käyttöoikeuksiin, joissa on ilmoitettu pääsyn estosta, suodatinohjelmien käytöstä ja valvontatoimista.

Näitä politiikkoja, ohjeita, määräyksiä ja käytäntöjä tulisi arvioida säännöllisesti.

## 2.3 Tietoisuuden lisääminen

Suodatinjärjestelmien rakentamisen lisäksi tai niiden sijaan on suositeltavaa, että käyttäjiä ja alaikäisten käyttäjien vanhempia valistetaan Internetin sisältämästä aineistosta.<sup>7, 8</sup> Tiedotuksen ja valistuksen avulla voidaan keskeisesti parantaa yksilön valmiuksia kohdata arveluttava tai kielletty materiaali, jolle käyttäjä voi tahtomattaan altistua käytettäessä ohjelmistoja tai laitteita, joissa suodatuspalveluja ei ole järjestetty, tai kun suodatuspalvelu on pystytty kiertämään tai se toimii puutteellisesti.

Erilaiset instituutiot ovat luoneet hyviä käytäntöjä, netikettejä<sup>9, 10</sup>, joita noudattaen käyttäjän tulisi toimia tietoverkoissa. Näiden yleisten käytäntöjen lisäksi on luotu lapsille ja nuorille omia netikettejä<sup>11, 12</sup>.

## 2.4 Viranomaismääräykset ja -suositukset

Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) suositus asiakaspäätteistä julkishallinnossa<sup>13</sup> suosittaa vain kirjastojen lastenosastoille lasten käyttöön asennettujen koneiden rajoittamista teknisin keinoin. Muuta liikennettä ei suosituksen mukaan tulisi rajoittaa. Suosituksessa ei ole kiinnitetty huomiota nuorison tietotekniikan käyttöön yleisemmin.

Suodatinjärjestelmä tulisi asentaa valtion tietohallinnon Internet-tietoturvallisuusohjeiden mukaisesti<sup>14</sup> ja sähköisen asioinnin tietoturvan yleisohjeen mukaisesti<sup>15</sup>, joka myös sisältää ohjeita järjestelmien hankintaan ja niiden yhteensopivuuteen. Samoin suodatinjärjestelmän tietoturvan pettäessä tulisi noudattaa vastaavia ohjeita.<sup>16</sup>

---

<sup>7</sup> <http://www.tietoturvakoulu.fi/>

<sup>8</sup> [http://www.mll.fi/kasvattajan\\_tietokulma/viisaasti\\_verkossa/tunnista\\_vaarat\\_ja\\_suojaa\\_lasta/](http://www.mll.fi/kasvattajan_tietokulma/viisaasti_verkossa/tunnista_vaarat_ja_suojaa_lasta/)

<sup>9</sup> [http://www.ficom.fi/fi/a\\_uutisaread.html?Id=982219844.html](http://www.ficom.fi/fi/a_uutisaread.html?Id=982219844.html)

<sup>10</sup> <http://www.internetopas.com/netiketti/>

<sup>11</sup> <http://www.pelastakaalapset.fi/nettivihje/saft-10-saantoa.php>

<sup>12</sup> <http://www.cybersmartkids.com.au/parents/general/>

<sup>13</sup> JUHTA, JHS 157, Asiakaspäätteet julkishallinnossa, 17.12.2004, voimassa 31.12.2006 saakka.

<sup>14</sup> Valtion Tietohallinnon Internet-Tietoturvallisuusohje, VAHTI 1/2003

<sup>15</sup> Sähköisen asioinnin tietoturvallisuuden yleisohje VAHTI 4/2001

<sup>16</sup> Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001

Suodatinjärjestelmän ylläpidossa ja varsinkin suodatettavan sisällön muutosprosessissa voidaan käyttää ohjeena valtion hallinnon sähköisen asiointipalvelun viitearkkitehtuuria.<sup>17</sup> Tämä asiakirja määrittelee sähköisen asiointipalvelun puitekehysten.

Suodatinjärjestelmän sisältämät säännöt ja sääntöjen sisältämät listat ja aineistot eivät ole tietoturvaluokiteltuja, eikä valtionhallinnon tietoturvaluokitellun aineiston käsittelyyn liittyviä ohjeistoja<sup>18</sup> näin ollen tarvitse noudattaa.

Mikäli suodatinjärjestelmä ostetaan palveluna tai sen päivittäminen on maksullista, tulee ottaa huomioon erityisesti ohjeet palvelujen ulkoistamisesta<sup>19</sup> ja niiden turvallisuudesta<sup>20</sup>.

## 2.5 Suodatuksessa huomioon otettavasta lainsäädännöstä

Suomen lainsäädännössä on varsin paljon säännöksiä, jotka määrittelevät jonkin sisällön kielletyksi tai jotka koskevat sisältöviestintää tietoverkoissa. Tällaiset säännökset on otettava huomioon harkittaessa suodatin- ja estojärjestelmien käyttöönottoa tai palvelujen hankintaa sekä laadittaessa järjestelmän käyttöohjeita ja käyttöehtoja.

### Sananvapaus ja rikoslain piirissä oleva aineisto

Perustuslain 12 §:ssä on turvattu sananvapaus. Sananvapauteen sisältyy muun muassa oikeus vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. Tarkempia säännöksiä sananvapauden käyttämisestä annetaan lailla. Lailla voidaan säätää kuvaohjelmia koskevia lasten suojelemiseksi välttämättömiä rajoituksia.

Mikäli kuvaohjelmaa ei ole kuvaohjelmien tarkastamisesta annetun lain nojalla hyväksytty esitettäväksi tai levitettäväksi tai sitä muuten ei ole tarkoitettu alaikäisten saataville, voidaan sen esittämisestä tai levittämisestä alaikäiselle tuomita rikoslain 17 luvun 18 b §:n mukaisesti sakkoo tai vankeutta. Myös muut rikoslain 17 luvun 18–20 §:n kriminalisoinnit suojaavat yleistä moraalista. Niiden suojaava vaikutus kohdistuu aikuisten ohella myös erityisesti lapsiin. Rikoslain säännökset ovat teknologianeutraaleja. Ne koskevat fyysisten kappaleiden hallussapidon, levittämisen ja esittämisen ohella myös Internetiin kytketyille tietokoneelle tallennettua aineistoa.

Tällä hetkellä pääsynestoa lapsipornoa sisältäville sivuille ollaan toteuttamassa operaattoreiden vapaaehtoisilla toimilla.

Tietojen tallennuspalveluja tarjoavalla palvelun tarjoajalla on tietoyhteiskunnan palvelujen tarjoamisesta annetun lain mukaan mahdollisuus rajoittaa tietynlaisten sisältöjen tarjoamista. Palvelun tarjoajalle voi syntyä jopa vastuu tallennettujen tietojen sisällöstä ja välittämisestä, mikäli palvelun tarjoaja ei estä pääsyä rikoslain 17 luvun 18 tai 18 a §:ien vastaisiin aineistoihin. Tallennuspalvelun tarjoajien tekemä sisällön suodatus on siten mahdollista vähintään niissä yksittäisissä ja tietoon tulleissa tapauksissa, joissa Internetissä levitetään sukupuolisiveellisyttä loukkaavia kuvia.

---

<sup>17</sup> Hallinnon sähköisen asiointipalvelun viitearkkitehtuuri, Valtiovarainministeriön työryhmämuistioita 34/2001

<sup>18</sup> VM:n Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje -ohje 5/01/2000, Ohjeellisesti: Valtion Tietohallinnon Arkaluonteiset kansainväliset tietoaineistot, Käsittelyperiaatteet valtionhallinnossa, VAHTI 4/2002,

<sup>19</sup> Valtionhallinnolla ei ole tietotekniikan ulkoistamiseen ohjeistusta. Valtion tietotekniikkahankintojen tarkistuslistan kappaletta 6 voidaan käyttää soveltuvin osin (VAHTI 6/2001). Sopimuksellisesti VYSEN erityisehdot käyttöpalveluista kattaa ulkoistetut palvelut.

<sup>20</sup> Valtion tietohallintotoimintojen ulkoistamisen tietoturvaluossuositus (VAHTI 2/1999)

On myös huomattava, että tietoverkkoja, tietoliikennepalveluja ja tietoverkkorikollisuutta koskevista säännöksistä voi aiheutua oikeudellisia seuraamuksia, mikäli suodatinjärjestelmän voidaan katsoa haittaavan viestintää ja tietoliikennettä ilman käyttäjien kanssa tehtyjä sopimuksia tai lain-säädännössä säädettyjä perusteita.

Myös Internetin globaali luonne on otettava huomioon. Suomen rikoslakia sovelletaan rajoitetusti Suomen rajojen ulkopuolella tapahtuvaan laittomaan toimintaan.

Liikenne- ja viestintäministeriön julkaisema ns. Railaksen raportti käsittelee teleyritysten toimesta tapahtuvan suodatuksen laillisuutta, ja esittelee kattavan listan rikoslaissa rangaistaviksi säädettyistä rikoksista, jotka perustuvat tai voivat perustua tietoverkoissa julkaistuun sisältöön<sup>21</sup>.

## Sähköisen viestinnän tietosuoja ja henkilötietolaki

Jos suodatinjärjestelmien valvonta ja sitä varten kerätty tieto sisältää tietoa henkilöstä tai henkilö on tunnistettavissa valvontatiedosta, joudutaan verkkopalvelun käyttöehdoissa tai muussa tiedoissa käyttäjän kanssa sopimaan kerättävästä tiedosta sähköisen viestinnän tietosuojalain ja henkilötietolain puitteissa.<sup>22</sup> Arvioitaessa sitä, onko henkilöön yhdistettävissä oleva tieto sähköisen viestinnän tietosuojalaissa tarkoitettu tunnistamistieto vai henkilötieto, ratkaisevaa on tiedon käyttötarkoitus. Jos tieto on yhdistettävissä luonnolliseen henkilöön mutta se ei liity viestien siirtämiseen, jakelemiseen tai tarjolla pitämiseen viestintäverkoissa, kysymyksessä on henkilötietolaissa määritelty henkilötieto. Henkilötietolaki on sähköisen viestinnän tietosuojalakiin nähden yleislaki. Henkilötietolakia sovelletaan, jos sähköisen viestinnän tietosuojalaista ei muuta johdu.

Esimerkiksi opetuksen järjestäjä voi olla sähköisen viestinnän tietosuojalaissa tarkoitettu yhteisötilaaja, joka tilaa viestintäpalvelun tai lisäarvopalvelun käyttäjän käytettäväksi. Käyttäjät voivat olla esimerkiksi oppilaitoksessa opiskelevat oppilaat. Yhteisötilaajana olevan oppilaitoksen on lain mukaan käsiteltävä teknisiin järjestelmiinsä kertyviä oppilaiden luottamuksellisia viestejä ja tunnistamistietoja (mukaan lukien Internet-sivujen selailusta kertyneet tiedot) siten, ettei viestinnän luottamuksellisuutta ja yksityisyyden suojaa loukata. Vaitiolovelvollisuudesta ja hyväksikäyttökiellosta säädetään lain 5 §:ssä.

Henkilötietolain soveltamisalaan kuuluvia henkilötietoja voivat olla esimerkiksi erilaisten tietojärjestelmien käyttämiseen oikeuttavien käyttöoikeuksien myöntämiseen ja hallintaan liittyvät tiedot. Käyttöoikeuksien myöntämisiä saattaa tapahtua esimerkiksi silloin, jos oppilaitoksen oppilaiden käyttämissä Internet-yhteyksissä suodatettaisiin viestintää mutta opettajien käyttämissä ei. Käyttäjille myönnettyihin käyttöoikeuksiin liittyvät tiedot talletetaan tätä tarkoitusta varten perustettuun henkilörekisteriin. Mikäli mahdollista, suodatin- ja estojärjestelmät tulisi toteuttaa henkilötietoja keräämättä.

Suunnitteluvaiheessa tulisi luoda toimintamalli sellaisia tilanteita varten, joissa käyttäjän havaitaan kiertävän suodatin- tai estojärjestelmää. Ennakolta mietitty toimintamalli estää kiertäjän tunnistamis- ja henkilötietojen loukkaamisen tilannetta selvitettäessä.

Jos tietojärjestelmässä käsitellään työntekijöiden henkilötietoja, myös laki yksityisyyden suojasta työelämässä tulee sovellettavaksi.

---

<sup>21</sup> Asianajotoimisto Krogeruksen selvitys liikenne- ja viestintäministeriölle lainsäädännöllisistä esteistä ja muutostarpeista rikollisen ja lapsille haitallisen sisällön estokeytojen velvoittavuuteen liittyen, 2005. Liite 1. <http://www.mintc.fi/oliver/upl973-Railaksen%20selvitys.pdf>

<sup>22</sup> Lisätietoa sähköisen viestinnän tietosuojasta Viestintäviraston verkkopalvelusta: <http://www.ficora.fi> ja henkilötietolaista tietosuojavaltuutetun verkkopalvelusta: <http://www.tietosuoja.fi>.

## Käytettävien aineistojen hankinta ja valinta

Sisältöjen suodattamisen oikeudellinen arviointi riippuu siitä, millä tasolla suodattaminen tapahtuu. Suodattamista voidaan tehdä tiedonsiirtopalvelujen tarjoajina toimivien välittäjien ohella myös Internetissä tapahtuvan viestinnän vastaanottajatasolla. Suodatin- ja estojärjestelmien tai niitä koskevien palvelujen hankkijat voivat järjestelmien avulla rajoittaa pääsyä niihin sisältöihin, joiden he eivät katso kuuluvan toiminnassaan käytettäviin aineistoihin.

Esimerkiksi kuntien kirjastoilla ja kouluilla on niitä koskevan lainsäädännön sekä viranomaismääräysten ja -ohjeistuksen rajoissa vapaus määritellä ne lasten kasvulle ja kehitykselle sopivat aineistot, joita käyttöönsä hankkivat.

Kirjastolain mukaan 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. Tämä ei tarkoita sitä, että kirjaston tulisi hankkia tai muuten mahdollistaa asiakkaidensa pääsy kaikkeen mahdolliseen olemassa olevaan aineistoon. Sama koskee oppilaitoksia.

Suodatinjärjestelmän hankintaan liittyviin kysymyksiin sovelletaan oikeustoimilakia, kauppalakia ja vahingonkorvauslakia. Myös laki julkisista hankinnoista tulee sovellettavaksi, mikäli lain kynnyksirajat ylitetään. Julkisen hallinnon tietohallinnon neuvottelukunta JUHTA on luetellut huomattavan kattavasti lainsäädännön<sup>23</sup>, joka koskee julkisten verkkopalvelujen tarjoamista. Tämä lainsäädäntö pätee osin myös suodatinjärjestelmiin.

---

<sup>23</sup> <http://www.jhs-suositukset.fi/intermin/hankkeet/jhs/home.nsf/pages/31A162B71BED9C19C22570350047C6E6>



# 3 Tekniset haasteet

## 3.1 Suodatuksen kattavuus

Internet-liikenne koostuu useista eri tietoliikenneprotokollista, joista yleisimmät liittyvät www-, sähköposti-, tiedostonsiirto- ja keskustelu-liikenteeseen. Vain www- ja sähköpostiprotokollat käsittävät rajallisen määrän protokollia, kun taas varsinkin tiedostonsiirto-protokollia voi olla useita. Kaikki protokollat eivät ole avoimia standardeja.

Nykyiset suodatinjärjestelmät pystyvät kattamaan tyypillisesti muutaman tietoliikenneprotokollan. Pääsääntöisesti suodatinohjelmat rajaavat Internetin www-sivuille (HTTP-, HTTPS-protokollat). Osa ohjelmistoista voidaan asentaa välimuistipalvelimiin. Tällaisten suodatinohjelmien kiertämistä varten on jo kehitelty keinoja ja ohjelmistoja, joita käyttämällä suodatinohjelmia pystytään kiertämään, ellei asennusta ole tehty tavalla, joka estää ohituksen.

Tällä hetkellä markkinoilla olevista suodatinjärjestelmistä vain muutamalla pystytään luomaan varsin kattava järjestelmä, jolla voisi hallita isoa osaa rajoitettavaa Internet-liikennettä. Jotta kattavaan suodatukseen päästäisiin, pitäisi järjestelmä yleensä koota erilaisista suodatinohjelmista tai järjestelmistä. On huomattava, että osa varsinkin vertaisverkkojen suodatuksen toteutusratkaisuksista estää koko protokollan käytön eikä vain pääsyä varsinaisesti kiellettyyn materiaaliin, jolloin ei itse asiassa enää suodateta liikennettä vaan estetään liikenne täysin.

- *Arveluttavaa materiaalia voidaan jakaa erilaisilla peer-to-peer -verkoilla, joista jotkut, esimerkiksi freenet-verkosto (<http://freenetproject.org/>) käyttää salausta tiedostojen jakoon. Suomessakin jopa lainvastaista materiaalia on saatavilla nntp-protokollalla (Usenet-uutiset) jaettuna suomalaisilla palvelimilla.<sup>24</sup>*

Joskus voidaan muita ohjelmia käyttää suodattamisessa tietyissä rajoissa ja täten parantaa suodatuksen kattavuutta. Yleisesti roskapostisuodatinohjelmia voidaan käyttää täydentävänä keinona estämään sähköpostissa tulevia kyseenalaisia roskaposteja. Roskapostisuodatinohjelmat eivät kuitenkaan yleensä estä käyttäjää saamasta haitallista sisältöä esimerkiksi toiselta käyttäjältä. Hakukoneissa voidaan myös käyttää sisäänrakennettuja suodatinohjelmia, jolloin epätoivottava materiaali ei näy hakukoneen tuloksissa. Tämä keino ei kuitenkaan kata kaikkia hakukoneita, ja sen pakottaminen päälle vaatii kohtuullisen hyvää tietämystä tietoverkkojen toiminnallisuudesta.

Verkkoteknisin keinoin pystytään kattavuutta parantamaan, mutta näiden keinojen automaattinen päivitys on haastavaa etenkin sellaisille yhteisöille, joiden tietotekniset voimavarat ovat rajallisia. Yleensä liikenteen rajoittamista pystytään toteuttamaan verkon liitoskohdissa reitittimin ja verkkojen reunoilla palomurein. Lisäksi on olemassa suodatinlaitteistoja, joiden kautta kaikki liikenne voidaan yhdistää kulkemaan tai liikenne ohjata uudelleen niille.

---

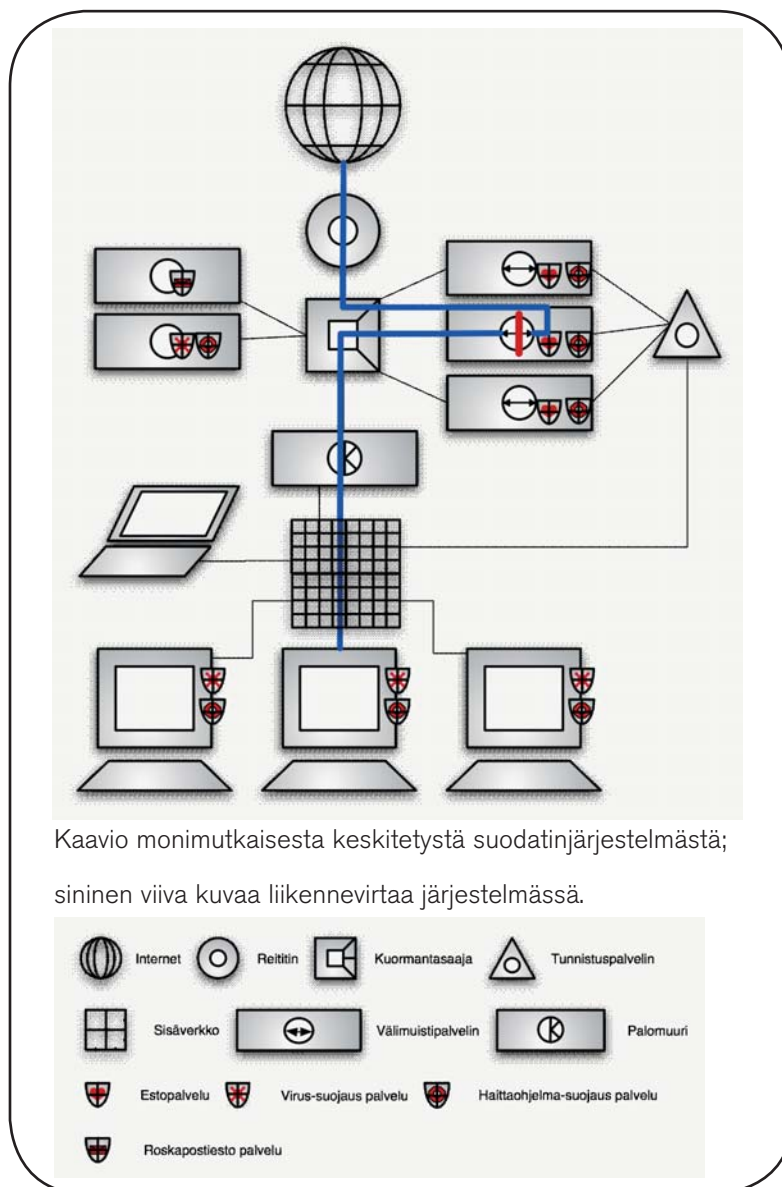
<sup>24</sup> (<http://www.helsinginsanomat.fi/tuoreet/artikkeli/1135218177727>).

Suodatusta ei voida toteuttaa lainkaan salatulle liikenteelle, joten ainoa estotoimenpide tähän tapaukseen on joko estää salatun liikenteen käyttö kokonaan tai rajoittaa sitä. Mikäli liikenne säädetään toimimaan toisin kuin se yleensä toimii, liikennettä ei voida havaita muuten kuin keräämällä verkon solmupisteistä kattavasti tietoa tai paljastamalla verkon väärinkäytöksiä verkon liikennettä kuuntelemalla.

- Mikäli salattu liikenne kielletään, voidaan käyttäjän tietoturva heikentää oleellisesti. Esimerkiksi verkkopankin käyttö voisi tulla helposti salakuunneltavaksi, ja altistaa käyttäjät jopa huomattaviin menetyksiin. Esimerkiksi vain muutaman salasanan selville saaminen aiheutti Nordean asiakkaille noin 60 000 euron menetyksen.<sup>25</sup>

Samoin kielletty materiaali voidaan siirtää käyttämään toista teknologiaa tai tietoliikenneprotokollaa, tai tiedostoja voidaan muokata niin, että niistä varsin vaivattomasti tulee käytännössä tunnistamattomia. Lisäksi käyttämällä suljettuja verkkoja voidaan suodatinjärjestelmiä helposti kiertää, sillä useimmiten suodatuslistan estokohde sisältää tiedon siitä, missä materiaali on.

Erilaisia teknisiä ja muita menetelmiä suodatuksessa on esitelty muun muassa liikenneministeriön raportissa<sup>26</sup>, joka käsittelee lapsipornon suodatusta.



<sup>25</sup> ([http://www.tietokone.fi/pda/uutinen.asp?news\\_id=25605](http://www.tietokone.fi/pda/uutinen.asp?news_id=25605)).

<sup>26</sup> <http://www.mintc.fi/oliver/upl984-Selvitys.pdf>

## 3.2 Suodatuksen yhteneväisyys

Mikäli yhteisö, jossa suodatusta järjestetään, hankkii järjestelmät hajautetusti eikä suositusta yhden järjestelmän käytöstä samoilla käyttöasetuksilla ole, on vaarana se, että saman yhteisön jäsenet eivät saa samanlaista palvelua, vaan eri käyttäjien välillä voi olla suuriakin eroja. Tyypillisesti merkittävät erot tulevat niistä päätöksistä, joilla määritellään, mitä eri suodatusluokkia valitaan.

Suomen kielen erityisluonne voi aiheuttaa myös suodatuksen yhteneväisyyteen eroja eri tuotteiden välillä. Kansainvälisten tuotteiden välillä ei ole merkittäviä eroja. Suurin osa tunnetuimmista estettävistä kansainvälisistä materiaaleista löytyy kaikkien toimittajien tuotteista, mutta suomalainen ja suomenkielinen haitalliseksi katsottu aineisto ei aina päädy kansainvälisten tuotteiden piiriin – ainakaan nopeasti. Usein ohjelmissa on mahdollisuus lisätä omia estokohteita, joilla voidaan korjata esimerkiksi suomenkielisten kohteiden puutteita.

- *Suomessa lasten alastomuus on luonnollinen asia, ja kuvia alastomista lapsista näkyy eri yhteyksissä. Yhdysvalloissa vastaavien kuvien esittämistä pidetään vähintäänkin arveluttavana.*

- *Erilaiset nimet kuten Rape, Kone, Aho, merkitsevät eri kielissä eri asioita, ja voivat näin joutua suodatetuksi ulkomaisella ohjelmistolla.*

- *Monasti myös aiheyhteyttä ei pystytä erikielisisä ohjelmistoissa ottamaan kattavasti huomioon. Tämä pätee erityisesti valistavaan ja lääketieteelliseen aineistoon.*

Myös kulttuuriset erot eri toimittajien järjestelmien kesken voivat aiheuttaa suodatinjärjestelmissä eroja. Esimerkiksi alastomuus on melko subjektiivinen käsite eri kulttuureissa.

## 3.3 Virheet suodatuksessa

Estokohteiden valitsemisessa voidaan käyttää erilaisia ohjelmistoja, jotka perustuvat ihmistyöhön, tekoälyyn, erilaisiin sääntöihin, tilastotieteeseen, kuvantunnistukseen tai muihin automaattisiin menetelmiin ja näiden yhdistelmiin, jolloin menetelmien puutteiden vuoksi pääsy sallittuun aineistoon voidaan kieltää.

- *Pelkän IP-osoitteen tai URL-nimen avulla tehtävä suodatus suodattaa koko sivuston, vaikka osa sivuston materiaalista voi olla täysin käyttöoikeuksien mukaista.*

- *Usein ns. villien korttien (wild card) avulla tehtävä suodatus voi suodattaa samoin suuren osan sivuston tavallisesta materiaalista.*

Käytännössä tämänlaatuiset virheet voidaan jälkikäteen korjata erilaisin menetelmin. Suodatinohjelmistojen toimittajat joko itse korjaavat tilanteen tai järjestelmän ylläpitäjä voi lisätä poikkeussäännön, jolla tilanne korjataan, mikäli ohjelmisto sallii ylimääräisten sääntöjen tai poikkeusten luonnin.

## 3.4 Suodatuksen ylläpito ja päivitys

Merkittävä osa suodatettavasta materiaalista on oikeudelliselta luonteeltaan melko vaihtuvaa joutuessaan siitä, että osa aineistosta rikkoo tekijänoikeuslainsäädäntöä tai yksityisyyttä, jolloin aineiston ylläpitäjät joutuvat poistamaan kaiken tai osan aineistostaan väärinkäytösten paljastuttua.

- *Joskus sama aineisto siirretään väärinkäytösten varalta toisaalle, mikä aiheuttaa vaihtuvuutta, samoin kun saman aineiston kopioiminen ja liittäminen uuteen materiaaliin. Materiaalia voidaan siirtää paikasta toiseen, ja välittäminen voidaan tehdä erilaisin tietoliikenneprotokollin. Erilaisia yksinkertaisia teknisiä keinoja kuten uudelleen nimeämistä ja pakkaamista käyttämällä samasta materiaalista voidaan luoda loputon määrä variaatioita.*

Nämä pakottavat suodatinohjelmien toimittajia ylläpitämään suodatinohjelmia säännöllisesti, lukuun ottamatta niitä toimittajia, jotka uskovat automaattiseen luokitteluun ja tekoälyyn.

Jos suodatinohjelman kattavuudessa on merkittäviä aukkoja johtuen esimerkiksi paikallisista vaatimuksista ja jos aukot tilkitään sisäisillä resursseilla, näitä korjauksia tulee ylläpitää jatkuvasti, jotta suodatinohjelman kattavuus pysyisi vaadittuna. Tällainen täydennystyö voi osoittautua oletettua työläemmäksi, eikä siihen tulisi ryhtyä kuin tapauksissa, joissa täydennyksen voidaan olettaa olevan pysyväisluontoinen.

Jatkuva ohjelmiston osien muutos aiheuttaa päivitystarpeen, joka tyypillisesti tehdään automaattisesti. Useimmiten uusi päivitys on käyttäjien saatavilla jopa useasti viikossa. Nykyään päivitysten koko voi olla merkittävä, jolloin päivitysten ajoituksen määrittely pitää tehdä huolella, jotta päivitys itsessään ei aiheuta rasitusta verkkoyhteydellä ja siten alenna tietoverkon käytettävyyttä.

### 3.5 Suodatuksen luokat

Suodatuksen kohteita voidaan yleensä määrittellä aihepiirien avulla, jotka kukin toimittaja itse on määritellyt. Lisäksi on kehitetty yhtenäisiä suodatinluokituksia, joiden pyrkimyksenä on toteuttaa toimittajasta riippumattomia yleisiä järjestelmiä, jotka yleisimmin liittyvät kohdekoneissa toimiviin järjestelmiin.

Luokitusta voidaan tehdä myös Internetin sisällölle sisällöntuottajien toimesta, jolloin suodatinohjelmat voivat käyttää valmista materiaalin luokitusta hyväkseen.

Eräs avoimista luokitusjärjestelmistä<sup>27</sup>, jolla sisällön tuottajat voivat luokitella sisällön, luokittelee aineiston seuraavasti:

- Alastomuus
- Eroottinen aineisto
- Väkivalta
- Alatyylinen kielenkäyttö
- Mahdollisesti ihmiselle haitalliset tavat tai teot
- Käyttäjän määrittelemä luokitus
- Aiheyhteys

Luokituksen tarkoituksena on määrittellä tarkemmin ne aineistot, joihin pääsyä ei katsota suotavaksi. Eräissä tuotteissa luokkia voi olla kymmeniä, kun taas toisissa ainoa luokka on lapsille sopimaton aineisto.

Mikäli luokitus ja pääsynvalvonta voidaan yhdistää, käyttäjäryhmäkohtainen luokitus voi sallia tietyille käyttäjille pääsyn ja kieltää osalta käyttäjistä pääsyn luokiteltuun materiaaliin, jolloin pystytään paremmin palvelemaan käyttäjiin kohdistuvia vaatimuksia.

Tämä selvitys ei suosittele minkään tietyn mediasisällön suodattamista. Suodatustarpeen arviointi, suodatuksen kohteiden valikointi ja suodatinmenetelmien valinta ovat sen asiana, joka tekee päätöksen suodatin- ja estojärjestelmien käyttöönotosta tai niitä koskevien palvelujen hankkimisesta.

---

<sup>27</sup> <http://www.icra.org/vocabulary/>

## 4 Tekniset vaatimukset suodatukselle

Jotta tekniset vaatimukset suodatukselle voidaan määrittää, tiedossa tulee olla estettävän aineiston laajuus ja se, kuinka pitkälle eri käyttäjien välinen suodatus halutaan toteuttaa. Aineiston laajuus voidaan määritellä antamalla ohjeet siitä, mitkä suodatusluokat tullaan estämään.

Lisäksi tulee määritellä suodatuksen kattavuus eli se, millaista liikennettä tullaan estämään ja miten kattavasti tämä liikenteen suodattaminen tullaan suorittamaan.

Vaatimukset liikenteen valvonnalle ja liikenteen aiheuttamien lokien säilömisestä ja seurannasta tulee määritellä ennen käyttöönottoa tai hankintaa, samoin kuin listojen ylläpitoon ja päivittämiseen liittyvät seikat.

Perusvaatimuksena tekniselle suodatukselle voi olla suodatinjärjestelmän täydellinen hallinta siten, että käyttäjällä tai tavallisella käyttäjällä ei ole mahdollisuuksia kiertää suodatinjärjestelmää. Tämä tarkoittaa sitä, että järjestelmän verkkoliittymän liikenne hallitaan siinä määrin, että tavoitteeksi asetettu kattavuus suodattamisessa tullaan saavuttamaan. Toisaalta voidaan asettaa päämääräksi se, että tavallisen käyttäjän tahaton käyttö estetään, jolloin järjestelmästä voidaan luoda kohtuullisin kustannuksin.

Perusvaatimuksen lisäksi suodatinohjelmiston lisäksi järjestelmään lisää järjestelmän kuormitusta. Niin ollen nykyisen järjestelmän kestävyys ja tuleva kuorma on syytä selvittää ennen suodatinjärjestelmän asennusta. Mikäli järjestelmästä ei ole olemassa tilastotietoa riittävän pitkältä aikaväliltä, on suositeltavaa, että suodatinjärjestelmä asennetaan koejärjestelmään ja tätä järjestelmää kuormitetaan normaalilla käyttökuormalla tai että suodatinjärjestelmä asennetaan osajärjestelmään, jossa sitä kokeillaan tavallisella järjestelmän käytöllä. Lisäksi suodatuslistojen päivitys voi aiheuttaa tietoverkon osiin lisäliikennettä.

Myös tietoverkon osien ja käyttäjien tietokoneiden tietoturvan tulisi olla riittävän hyvässä kunnossa, jotta tietokoneisiin kohdistuvat muut uhat kuten kaappariohjelmat eivät käyttäisi tai murtaisi tai kiertäisi suodatinjärjestelmiä. On mahdollista, että turvatoimia laiminlyötyessä koneisiin itsessään voidaan asentaa materiaalia, joka ei ole sallittua. Lisäksi tietokoneiden käyttöoikeuksiin tulisi kiinnittää huomiota, jotta vihamielisten käyttäjien toimet voitaisiin minimoida mahdollisimman hyvin.

# 5 Nykyiset tekniset ratkaisut

## 5.1 Toimintaperiaate

### Listoihin perustuvat järjestelmät

Listoihin perustuvat järjestelmät sisältävät suodatettavien materiaalien listoja, joiden avulla suodatus tapahtuu. Lisäksi listat sisältävät suodatusluokittelun, jolla kiellettävien kohteiden valinta voidaan rajata sopivaksi.

Listat sisältävät yleensä tiedon siitä, missä estettävä materiaali on. Yleensä niissä ei oteta kantaa siihen, mitä materiaalia sivustossa tarkalleen ottaen on, vaan oletetaan, että tietty sivusto yleensä sisältää tietynlaista materiaalia, johon pääsy tulee kieltää paikan perusteella.

- *Esimerkkinä klassisin lienee [www.playboy.com](http://www.playboy.com), jonka sisällön asiallista osaa ei yleensä osata keskusteluissa kaivata. Osa täysin asiallisista sivustoista voi kuitenkin sisältää myös varsin arveluttavaa materiaalia, josta esimerkiksi USENET-uutisryhmästä lienee varsin tunnettu esimerkki. Alt-kategoria uutisissa voi sisältää kaikkea maan ja taivaan väliltä.*

Listoja päivitetään säännöllisesti, jotta suodatus pysyisi kattavana jatkuvasti. Listojen päivittäjät kuitenkin voivat olla joko toisesta kulttuurista, jolloin osa suomalaisesta sivustoista voi jäädä kattamatta, tai osa suomalaisia sivustoja voidaan sulkea niiden sisältämien suomalaisten sanojen vuoksi, joita ulkomaalaiset eivät pysty tulkitsemaan oikein. Suomalaisia päivittäjä-resursseja voi olla lukumääräisesti huomattavasti vähemmän kuin kansainvälisesti toimivien resurssien, ja näin osa Internetistä ei välttämättä tule katettua. Listat joka tapauksessa tulevat päivittymään viiveellä, joten on aina mahdollista, että käyttäjä pääsee johonkin haitalliseen materiaaliin.

### Luokitteluun perustuvat järjestelmät

Luokitteluun perustuvat järjestelmät perustuvat suodatuksen sisällöntuottajien tekemään vapaaehtoiseen luokitukseen.

- *Luokitteluun perustuva järjestelmä on käytössä British Telecomilla Iso-Britanniassa.*

Ohjelmistosta voidaan valita suodatusluokat, joilla suodatus tarkennetaan sopivaksi. Järjestelmää ei tarvitse periaatteessa päivittää lainkaan, vaan sisällöntuottaja vastaa päivityksistä.

Tällä hetkellä sisällöntoimittajista vain pieni osa on luokitellut materiaalin. Varsinkin vertaisverkkojen ja jutustelu-ohjelmien kautta tulevaa materiaalia ei ole luokiteltu lainkaan, ja näistä tuleva aineisto voidaan myös luokitella tahallisesti harhaanjohtavaksi.

## Tekoälyyn ja säännöstöihin perustuvat järjestelmät

Tekoälyyn ja säännöstöihin perustuvat järjestelmät pystyvät periaatteessa analysoimaan ja tosiaikaisesti päättämään sisällön sen sisältämän tiedon perusteella. Järjestelmiä voidaan myös opettaa etukäteen tunnistamaan tietynlaista paikallista aineistoa, jotta sen kattavuus olisi parempi.

Osa järjestelmistä pystyy jopa analysoimaan kuvatiedostoja ja päättämään esimerkiksi, sisältääkö kuva alastomuutta.

- *Automaattisiin järjestelmiin liittyvät ongelmat ovat moninaiset ja liittyvät materiaalin luokitteluun. Kuvan tunnistamisessa passikuvassa on yhtä paljon paljasta ihoa näkyvissä kuin alastonkuviissa. Seksuaalivalistus on termistöltään samankaltainen kuin kiellettävä materiaali muutenkin. Näiden asiayhteyksien havainnoimiseen tekoäly ei tällä hetkellä tarjoa kovinkaan luotettavaa keinoa, jolloin erikoissääntöjen ja poikkeuksien tekemiseen tulee olla resursseja riittävästi.*

Järjestelmää ei tarvitse päivittää lainkaan lukuun ottamatta ohjelmiston ylläpitoa, jolla pyritään varmentamaan se, että uusilla keinoilla ei järjestelmää voida ohittaa.

## 5.2 Toteutustapa

### Hajautetut järjestelmät

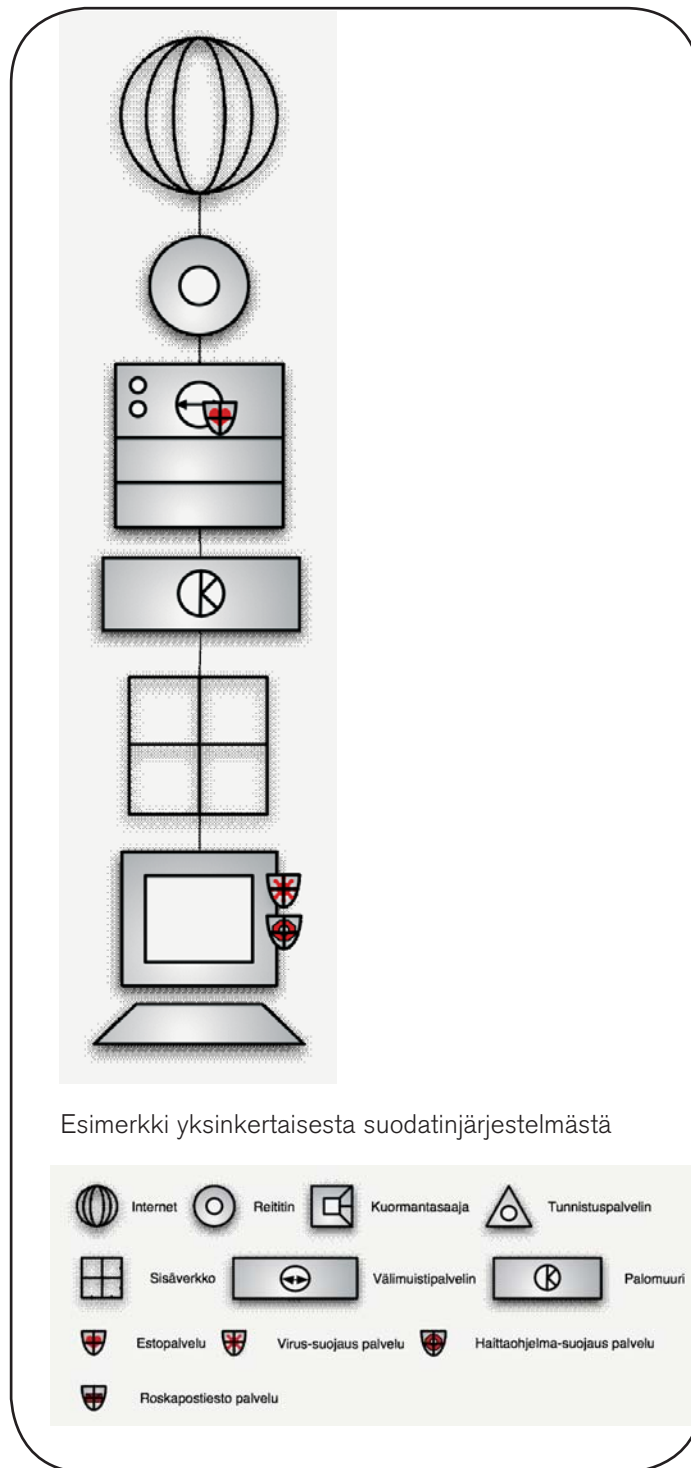
Pisimmilleen vietyinä hajautettu suodatinjärjestelmä asennetaan jokaiseen tietokoneeseen ja räätälöidään jokaiselle käyttäjälle tai käyttäjäryhmälle erikseen joko automaattisesti tai käsin. Tietokoneen muita asetuksia joudutaan muokkaamaan, jotta suodatinjärjestelmä toimisi oikein.

Kotikäyttöön tarkoitetut ohjelmistot toimivat tällä periaatteella. Samoin virusohjelmistoihin lisätyt suodatinohjelmistot ja -järjestelmät sekä käyttöjärjestelmätason suodatinohjelmistot ja järjestelmät toimivat käyttäjien tietokoneissa.

Hajautetuksi järjestelmäksi voidaan katsoa myös verkon osille tehtävät suodatustoimenpiteet, jolloin suodatinohjelmisto tai -laitteisto on käytännössä sama kuin keskitetty järjestelmä, mutta se voidaan mitoittaa pienemmäksi kuin silloin kun kaikki verkon liikenne johdetaan yhden solmukohdan kautta.

Jotta hajautettujen järjestelmien päivittäminen ei aiheuttaisi ylimääräistä kuormitusta, päivitysten ajoittaminen pitää tarkoin suunnitella niin, ettei normaali käyttö häiriinny ylimääräisestä liikenteestä.

Lisäksi hajautettuja järjestelmiä varten pitää olla mahdollisuus keskitettyyn hallinointiin, jotta varsinkin suurissa organisaatioissa järjestelmän asetusten muuttamiseen ei mene kohtuuttomasti aikaa ja resursseja. Varsinaisessa asennuksessa on kuitenkin mahdollista, että ohjelmistot joudutaan asentamaan yksi kerrallaan joka laitteeseen, mikäli käyttöjärjestelmäympäristöä ei ole asennettu tukemaan keskitettyä asennusta ja mikäli ohjelmisto itse ei sitä tue ja ohjelmiston muuntaminen etäasennettavaksi ei ole käytännöllistä.



## Keskitetyt järjestelmät

Keskitetyt järjestelmät asennetaan toimimaan verkon Internet-liittymäpisteiden läheisyyteen, jolloin kaikki Internetiin menevä ja sieltä tuleva liikenne tarkistetaan solmupisteessä. Keskitetyt järjestelmät sopivat erityisesti julkisyhteisöjen ja muiden sellaisten käyttäjien tarkoituksiin, joissa on kysymys laajemmista käyttöympäristöistä.

Keskitettyjen järjestelmien etuna voidaan pitää helppoa järjestelmän ylläpitoa ja tehokasta järjestelmän päivittämistä.



Järjestelmissä voi olla myös ylimääräisiä hyödyllistä toiminnallisuutta kuten virustorjuntaohjelmistoja.

## Suodatuspalvelut

Suodatuksen voi myös ostaa palveluna Internet-palvelun tuottajalta, jolloin järjestelmän ylläpito- ja päivitystyö on palveluntarjoajan vastuulla.

- *Suurimmat Internet-palveluntarjoajat tarjoavat suodatuspalveluja asiakkailleen.*

Palvelun ostajalla ei ole käytännössä paljonkaan mahdollisuuksia valita sitä, miten kattava suodatuksesta tulee.

Palvelun tarjoajaa voidaan vaihtaa melko vaivattomasti, eikä palvelua ostavan yhteisön tarvitse sioutua lisenssi- ja/tai laitekuluihin. Päivityksen vaatima verkkokapasiteettikin vapautuu käyttäjille.

## 5.3 Ilmaiset järjestelmät

Suodatinjärjestelmä voidaan rakentaa ilmaisista ohjelmistoista<sup>28</sup>, ja niiden toiminnallisuudesta saadaan samankaltainen kuin kaupallisista tuotteista.

Merkittävin ero ilmaistuotteissa on listojen päivittäminen, ja ilmaiset listat ovatkin merkittävästi kaupallisia tuotteita suppeampia, joten suodattamisen kattavuus voi olla tarpeisiin nähden vaillinaisen.

Eräs ilmaisista tuotteista<sup>29</sup> on luokitteluun perustuva järjestelmä, jolloin päivittämistä ei tarvita. Ohjelmisto estää pääsyn niihin kohteisiin, joissa ei ole sopivaa luokitusta. Lisenssi kuitenkin oikeuttaa vain kotikäyttöön.

## 5.4 Espoo esimerkkinä: Tietoliikenteen rakentamisesta Internetin sosiaalisiin pelisääntöihin

Esto- ja suodatinjärjestelmien käyttöönotto on käyttäjän kannalta varsinkin laajemmissa käyttöympäristöissä erittäin vaativa tehtävä. Se edellyttää järjestelmien erillisiin toimintoihin perehtymistä ja omien tarpeiden kartoittamista. Järjestelmän käyttöönotto edellyttää riittävää ja tarpeeksi pitkäkestoisista asiantuntijavoimien panostamista hankkeeseen.

---

<sup>28</sup> Tietokone 7-8.2005, sivu 63, Ratkaisut: Tee-se-itse-suodatus

<sup>29</sup> <http://www.icra.org/icraplus/>

Järjestelmien käyttöönotossa ollaan Suomessa monilla tahoilla kokemusten hankinnan alkuvaiheessa. Hyvän esimerkin siitä, millaisista askeleista ja toimenpiteistä järjestelmällisesti suunniteltu käyttöönotto voi koostua, on Espoon kaupungin opetustoimi. Työtä hankkeen parissa on tehty useita kuukausia.

### **1. Tietoliikenne**

Espoon suomenkielisen opetustoimen tavoitteena on ollut liittää kaikki oppilaitokset tietoliikenneverkon avulla Internetiin. Tavoitteena on ollut tarjota opiskelijoille Internetin sisältöjä, tietokantoja ja -lähteitä oppimisen tueksi.

### **2. Tietoliikennekapasiteetti**

Tietoliikenteen määrän lisääntyminen Internetin sisältöjen määrän ja erilaisten verkkopalvelujen käytön lisääntymisen kautta asettavat haasteen tietoliikennekapasiteetin riittävyydelle.

Monimedialaiset ja vuorovaikutteiset sisällöt vaativat tietoliikenteeltä aiempaa suurempaa kapasiteettia.

### **3. Tietoturva**

Tietoliikenteen rakentamisen yhteydessä on ratkaistu tietoliikenteen tietosuojaan ja -turvaan liittyviä kysymyksiä.

### **4. Virustorjunta**

Tietoliikenteen ja Internetin käytön riskeinä ovat erilaiset virukset ja haittaohjelmat. Näiden haittojen estäminen virus- ja haittaohjelmatorjunnalla on jatkuva ylläpitotyö.

### **5. Tiedonhallintataidot**

Internetin sisältöjen määrän lisääntyminen asettaa oppijan tiedonhaku- ja -hallintataidoille haasteita. Opetushenkilöstön täydennyskoulutuksessa tiedonhallintataitojen kehittämällä on keskeinen sija.

### **6. Portaalit tiedon ovina**

Internetin sisältöjen järjestämisessä on koottu erilaisia portaalreja, joiden tehtävänä on ollut koota yhteen tiettyyn aihepiiriin liittyviä aineistoja tai toimijoita.

### **7. Nettietiketti**

Internetin vuorovaikutteisten toimintojen hyödyntäminen edellyttää toimijoilta käyttäytymis- ja toimintasääntöjä. Nettietiketti-ohjeistuksella on pyritty luomaan rakentavia toimintatapoja Internetin vuorovaikutus- ja viestintätilanteisiin.

### **8. Internetin turvallisten sisältöjen valikointi**

Virus- ja haittaohjelmien rinnalle on otettu koekäyttöön erilaisia teknisiä Internetin sisällön suodatinjärjestelmiä. Tavoitteena on turvata Internetin sisällöt oppijoille sopiviksi ja turvallisiksi.

### **9. Sähköinen oppimisympäristö**

Sähköisen oppimisen tueksi Espoossa on otettu käyttöön kaikille yhteinen sähköinen oppimisympäristö, joka tarjoaa mahdollisuuden erilaisten lähde- ja linkkilistojen kokoamiselle. Opetushenkilöstö voi tarjota oppijoille etukäteen valikoituja hyviä oppisisältöjä sähköisen oppimisympäristön kustannettujen sisältöjen rinnalle.

Sähköinen oppimisympäristön on suljettu ympäristö, johon tarvitaan henkilökohtainen kirjautumistunnus.

### **10. Internetin sosiaaliset pelisäännöt**

Internetin pelilliset vuorovaikutteiset sisällöt ja toiminnot edellyttävät yhteisiä hyväksytyjä pelisääntöjä. Nämä pelisäännöt tullaan päivittämään Nettietiketin ohjeistuksiin.

# 6 Tulevaisuuden ratkaisuja

## 6.1 Automaattinen sisällönhallinta

Automaattisilla sisällönhallintaratkaisulla pyritään tekoälyn, sääntöjärjestelmien ja erilaisten tekstin- ja kuvantunnistusmenetelmien avulla joko dynaamiseen tosiaikaiseen tunnistamiseen tai listapohjaiseen järjestelmän automaattiseen täydentämiseen, jolloin myös käyttäjiltä tulevat muutospyynnöt voidaan tällaisilla järjestelmillä esikäsitellä tai automatisoida tarvittaessa.

## 6.2 Keskitetyt sisällönhallintajärjestelmät

Sisällönhallintajärjestelmien tarkoitus on tehostaa suodatinjärjestelmien tukitoimia, kuten sisällön hallinnan päätöksiä ja niiden läpinäkyvyyttä, muutosten läpimenoaikoja, ja parantaa erilaisten sisältöön vaikuttavien organisaatioiden tiedonkulkua.

Lisäksi hallintajärjestelmillä voidaan valvoa erilaisten suodatinjärjestelmien toimintaa ja listojen ajantasaisuutta.

## 7 Hankinnassa ja käyttöönnotossa huomioon otettavia näkökohtia

Kun järjestelmää suunnitellaan, tärkeää on määrittää täsmällisesti sen käyttötarkoitus ja tavoitteet – erityisesti päätös siitä, kuinka kattava järjestelmän tulisi olla, jotta järjestelmä voidaan rakentaa asianmukaisesti täyttämään juuri ne vaatimukset, jotka halutaan. Kun ymmärretään, mihin tarkoitukseen järjestelmä rakennetaan, voidaan päästä kohtuullisiin kustannuksiin järjestelmää rakennettaessa ja etenkin sitä ylläpidettäessä. Mikäli vaatimukset ovat puutteelliset, voidaan päätyä järjestelmään, joka on laiton tai toimii vain tietyn hetken tarkoituksenmukaisesti, ja silti ne käyttäjät, joita varten järjestelmä suunniteltiin, pystyvät kiertämään sen helposti.

Tämän asiakirjan liitteeseen on laadittu muistilista hankinnan helpottamiseksi.

On huomattava, että järjestelmää, jota käyttäjä ei pysty kiertämään helposti on vaikea rakentaa, ja osaan haitallista materiaalista voi käyttäjä joka tapauksessa päätyä tahattomastikin.

Tekninen toteutus tulisi tehdä niin, että suodatinjärjestelmää ei pyrittäisi piilottamaan vaan että järjestelmä ilmoittaisi selkeästi niissä tapauksissa, jolloin materiaaliin ei päästä. Näin käyttäjä voi pyytää muutosta erheellisestä suodatuksesta. Toteutuksen ei tulisi myöskään aiheuttaa riskejä varsinaiselle palvelulle tai sen tasolle.

Vaikka järjestelmä on tekninen, riittävästi resursseja tulisi varata tiedottamiseen ja suodatusten muutosten tekoon. Suodatuksen hallinnointi ja suodatusperusteet tulisi kuvata selkeästi, ja tämän tiedon tulisi olla julkista. Käyttäjien tulisi aina olla tietoisia palvelun käyttöehdoista, joissa suodattaminen tulisi mainita riittävän tarkasti. Muutosten ehdottaminen tulisi voida tehdä vaivattomasti ja läpinäkyvästi, ja ne tulisi toteuttaa kohtuullisessa ajassa. Kieltävät päätökset tulisi aina perustella riittävän selkeästi, jotta vältetään turhautumilta palvelujen käytössä.

Jotta suodatinjärjestelmä säilyisi toimintakykyisenä, on riittävä määrä resursseja varattava sen ylläpitämiseen ja ajantasaisena pitämiseen. Tämä voi merkitä järjestelmän uusimista säännöllisin väliajoin, varsinkin sellaisissa tietoverkoissa, joissa käyttäjien ja liikenteen määrät kasvavat jatkuvasti. Samoin ylläpitohenkilökunnan kouluttamiseen tulisi varata riittävästi varoja. Myös suodatinohjelmiston kyky pitää itsensä ajantasaisena on varsin tärkeää toimintakyvyn kannalta.

Suodatinjärjestelmän rakentaminen voi olla kallista ja sen ylläpito saattaa viedä rajallisista resursseista merkittävänkin osan. Tällöin saattaa olla aiheellista harkita suodattamisen hankkimista palveluna. Mikäli suodatus hankitaan palveluna, hankintapäätöstä tehtäessä on otettava huomioon se, millaisen palvelun palveluntarjoaja kykenee tarjoamaan, pystyykö palveluntarjoaja tekemään palvelustaan riittävän läpinäkyvän ja kattavan organisaation tarpeisiin ja toteutuvatko laillisuusvaatimukset, kun järjestelmä on toisen hallinnoima palvelu. Palvelun sisältöön ja palvelun laadun takaavaan palvelutasosopimukseen on syytä kiinnittää erityistä huomiota.

# Liite. Suodatinjärjestelmien hankinnan muistilista

## Taustatietoa

Hankinnasta päätettäessä ja sitä arvioitaessa voidaan käyttää apuna soveltuvin osin erilaisia valtionhallinnon ohjeita tietotekniikan hankinnoista.<sup>30</sup>

Mikäli suodatinjärjestelmää harkitaan asennettavaksi, on hyvä kerätä tietoja siitä, miten Internetiä tietoverkossa käytetään. Erilaiset lokit kuten välityspalvelinten, reititinten ja palomuurien lokit voivat jopa paljastaa, että tarvetta suodatinjärjestelmän käyttöön ei ole, jos lokeihin ei ole tallentunut vierailuja epätoivottaviin kohteisiin. Sähköisen viestinnän tietosuojaja henkilötietolaki on otettava huomioon tietoja kerätessä.

Sopimuksissa tulisi käyttää valtion tietotekniikkahankintojen yleisiä sopimusehtoja.

## Hankinnan esitietoja

Mikä on järjestelmän käyttötarve?

- Keitä käyttäjiä järjestelmä koskee?
- Mitä tietoja käyttäjä ei saa päästä näkemään?
- Mitä tietoliikennettä pääasiassa estetään (HTTP, HTTPS, muut protokollat)?
- Kuka päättää, mikä aineisto on sallittu ja mikä kielletty?

Miten paljon järjestelmä kuluttaa teknistä infrastruktuuria muuten?

- Miten paljon päivitykset käyttävät verkkokapasiteettia?
- Voidaanko käyttää osin olemassa olevia palvelimia tai tietokoneita?
- Mikäli järjestelmä asennetaan olemassa oleviin tietokoneisiin tai järjestelmiin, miten lisäkuormitus vaikuttaa muihin palveluihin?
- Joudutaanko palvelun vuoksi uusimaan työasemia, palvelimia tai järjestelmiä?

Mitä muutoksia olemassa oleviin tietojärjestelmiin joudutaan tekemään uuden palvelun saattamiseksi toimintakykyiseksi?

- Joudutaanko verkon reititystä muuttamaan?
- Joudutaanko pääsilystoja muuttamaan tai lisäämään?
- Joudutaanko verkkorakennetta muuttamaan?
- Joudutaanko palomuurisääntöjä muuttamaan?
- Joudutaanko politiikkoja ja muita teknisiä asiakirjoja päivittämään, täydentämään tai lisäämään?
- Joudutaanko valvontajärjestelmiin tekemään muutoksia?
- Kuka vastaa muutoksista?
- Kuka tekee muutokset?

---

<sup>30</sup> Julkisten Verkkopalvelujen Laatuksiteerit, Valtiovarainministeriön hallinnon kehittämissosasto, 8/2004

Valtion Tietotekniikkahankintojen Tietoturvallisuuden Tarkistuslista, Valtionhallinnon tietoturvallisuuden johtoryhmä, 6/2001

<http://www.vm.fi/vm/liston/page.lsp?r=16828&l=fi>

<http://www.vn.fi/vm/kehittaminen/tietohallinto/vati/sopimusedot1998.pdf>

Mitä muutoksia järjestelmään tulee tehdä, jotta se vastaa paikallisia tarpeita?

- Minkälaiset paikalliset virheilmoitukset tulee järjestelmään luoda?
- Mitä tietoa valvontajärjestelmiin haetaan?
- Miten järjestetään palautetiedon kerääminen?
- Tarvitaanko järjestelmää varten verkkosivustoa, joka ohjeistaa muutoksien haussa ja kertoo sisällön hallinnan politiikoista?

Mihin laitteet sijoitetaan verkkotopologiassa?

Missä on laitteiden fyysinen sijainti ja niiden vaatima tila- ja sähkön tarve sekä vaikutus ilmastointiin?

Kuka vastaa laitteiden ja ohjelmistojen ylläpidosta?

- Minkälaista koulutusta tarvitaan, jotta organisaatio kykenee ylläpitämään järjestelmää?

Kuka vastaa paikallisen aineiston päivytyksestä ja muutoksista?

Kuka vastaa tiedotuksesta ja tiedotusmateriaalista?

### **Koekäytön mahdollisuus**

On suositeltavaa asentaa järjestelmä koekäyttöön ennen hankkimista ja tutustua sen suorituskykyyn, käytettävyyteen ja ylläpidettävyyteen.

### **Toimittajasta**

Onko toimittaja vakavarainen ja tunnettu tekijä tällä alalla?

Kuinka monta vastaavan kokoista samanlaista järjestelmää toimittaja on toimittanut viimeisten vuosien aikana?

### **Järjestelmän hankinnan tunnuspiirteitä**

Miltä materiaalilta käyttäjä tulee suojata?

Minkä tasoista suojausta organisaatio kaipaa?

- Joudutaanko ohjelmiston sijasta asentamaan järjestelmä, joka vaatii huomattavaa ylläpitoa
- Joudutaanko suodatuslistaa itse päivittämään, jotta se vastaisi suomalaisia vaatimuksia ja kulttuuria?

Minkä kokoinen on suojattava järjestelmä?

- Kuinka monta samanaikaista käyttäjää?
- Kuinka monta tietokonetta?
- Kuinka monta laitetta tarvitaan?

Millainen saatavuus järjestelmällä tulee olla?

Milloin palvelun täytyy olla toiminnassa?

- Arkipäivisin
- Päivisin
- Päivisin ja iltaisin
- Ympäri vuorokauden

Rakennetaanko järjestelmä toimimaan yhdyskäytävänä, jolloin järjestelmän luotettavuus pitää olla suurempi kuin sellaisilla suodatinohjelmistoilla, jotka asennetaan paikalliseen tietokoneeseen?

Miten järjestelmää pystytään laajentamaan, mikäli tietoliikennemäärät kasvavat ratkaisevasti?

Millainen elinkaari järjestelmällä on, milloin vastaava korvausinvestointi tulee budjetoida, vai tulaaanko järjestelmää uusimaan sitä mukaa kuin liikennemäärät kasvavat?

Mihin järjestelmän hinta perustuu?

- Millainen lisensiointipolitiikka järjestelmällä tai ohjelmistolla on?
- Mikä on laitteiden ja ohjelmiston osuus toimituksesta?
- Mitä asiantuntijatyötä tehdään toimituksen yhteydessä?
- Mitkä ovat järjestelmän kuvaavat asiakirjat?
- Mitkä ovat toimitukseen kuuluvat asiakirjat?

Mikä on laitteen suunniteltu tukitarve?

- Tarvitaanko varaosia vai luotetaanko toimittajan kykyyn toimittaa uusi tilalle tai korjata laite sovitussa ajassa?
- Miten järjestelmän konfiguraatiodostot varmuuskopioidaan?
- Mihin järjestelmän lokit kerätään, ja kuinka pitkän aikaa lokitietoja pystytään säilyttämään?

Minkälaisen tuen ja takuun toimittaja antaa järjestelmälle?

- Mitkä ovat vasteajat eri vikailmoituksille?
- Kuinka nopeasti toimittaja kykenee korjaamaan laitteen?
- Mitä tapahtuu, jos laitteistoa ei kyetäkään korjaamaan määräajassa?
- Millaiseen takuuseen tukipalvelujen laadusta toimittaja on valmis sitoutumaan?

Miten järjestelmää hallitaan, ja voidaananko sitä etähallita, ja voidaananko järjestelmä liittää organisaation hallintajärjestelmiin, vai tuleeko järjestelmän mukana omat hallintatyökalut?

Kuinka järjestelmä otetaan käyttöön?

- Mikä on käyttöönottoaikataulu ja -suunnitelma?
- Mitä resursseja vaaditaan käyttöönotossa asiakkaalta?
- Kenen vastuulla on käyttöönotto?
- Käytetäänkö asennuksissa alihankkijoita?



OPĒTUSMINISTERIŅĀ

*Undervisningsministeriet*

MINISTRY OF EDUCATION

*Ministère de l'Éducation*

ISBN 952-485-100-8 (pdf)  
ISSN 1458-8102