EDUSKUNNAN
APULAISOIKEUSASIAMIES

Helsinki 7.6.2010

VM 047:00/2007
08. 06. 2010

Dnro 1869/5/10

Valtiovarainministeriö
Hallinnon kehittämisosasto
PL 28
00023 Valtiovarainministeriö

Viite: Lausuntopyyntönne 21.5.2010

LAUSUNTO

Valtiovarainministeriö on pyytänyt kirjeellään ministeriöiden, virastojen ja laitosten, muun ohella eduskunnan oikeusasiamiehen, lausuntoa koskien luonnosta valtionhallinnon tietoturvallisuuden kehittämisohjelmaksi vuosille 2010–2015 (VAHTI 19.5.2010). Lausuntonani esitän kohteliaimmin seuraavan.

1) Kehitysohjelman sisällön, toimenpiteiden, painotusten ja toimeenpanon yleinen arviointi

Tietoturvallisuutta koskevasta ohjeistuksesta on yhteiskunnan verkottumisen ja kansainvälisten tietoverkkojen myötä tullut laajeneva, monimutkainen ja osin vaikeaselkoinenkin säädös-, ohje-, suositus- ja sopimuskokonaisuus (vrt. http://www.vm.fi/vm/liston/page.lsp?r=2685&l=fi). Tietoturvallisuusasioissa on ollut ongelmallista myös ohjeiden ymmärrettävyys ja yleiskielelle vieras termistö. Pääosa viranomaisten tietoturvallisuusaineistoista on kylläkin saatavilla julkisina asiakirjoina tai valtiovarainministeriön hallinnon kehittämisosaston kotisivulla internetissä (ks. http://www.vm.fi/vm/fi/hakutulos.jsp?query=Vahti&perushaku=1). Valtioneuvosto on hyväksynyt jo syyskuussa 2003 kansallisen tietoturvastrategian, jonka toimeenpanosta on vastannut tietoturvallisuusasioiden neuvottelukunta. Tietoturvallisuus on nykyisin kytketty myös organisaation uskottavuuteen ja palveluiden laatuun (vrt. Vahti 2/2004).

Nyt puheena olevaan kehittämisohjelmaan sisältyy kahdelle hallituskaudelle jakautuvia mittavia, poikkihallinnollisiakin toimenpiteitä. Kehitysohjelman luonnoksesta ilmenevät ohjelmakauden 2010–2015 tärkeimmät tavoitteet: tietoturvallisuuden konsernitason keskittäminen valtiovarainministeriöön, tietoturvasuositusten sitovuuden lisääminen sekä kunkin tietotekniikkaa käyttävän organisaation vastuiden ja osaamisen lisääminen. Meneillään on muutoinkin kehittämistoimet valtion konserniohjauksen tiivistämiseksi, erityisesti tietohallinnon osalta. Näihin yleisiin tavoitteisiin ei ole laillisuusvalvonnan kannalta sinänsä huomauttamista, vaikka valtiota organisaationa ja työpaikkana ei perustuslaissa (731/1999) ja laissa valtioneuvostosta (175/2003) säädösteknisesti konsernina pidetäkään.

Osoite: 00102 Eduskunta
Puhelin 09-4321
Telefax 09-432 2268
Sähköposti: eoa-kirjaamo@eduskunta.fi
Internet: http://www.oikeusasiamies.fi

Perustuslain (731/99) 22 §:n mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen. Tietoturvallisuuden kautta turvattavia perusoikeuksia ovat erityisesti perustuslain 10 §:n mukainen yksityiselämän suoja ja perustuslain 12 §:ssä säädetyt sananvapaus ja julkisuus. Julkishallinnon verkkopalveluissa on otettava huomioon kansalaisten yhdenvertaisuuden ja hyvän hallinnon vaatimukset. Koska eduskunnan oikeusasiamiehen tehtäviin kuuluu perustuslain 109 §:n mukaan laillisuusvalvonta, on erääksi kehittämisohjelman tavoitteeksi asetettu tietoturvallisuuden lainsäädännön kehittäminen sinänsä kannatettava pyrkimys.

Eduskunnan entinen oikeusasiamies Riitta-Leena Paunio on jo 31.5.2005 lausunnossaan oikeusministeriölle todennut tietoturvallisuuteen liittyvistä laillisuuskysymyksistä (EOA dnro 1978/5/05; Paremman sääntelyn toimintaohjelma), että julkinen hallinto toimii enenevässä määrin sähköisen tiedon varassa. Kyseessä on merkittävä hallinnon muutos, jossa oikeusturvanäkökohtia ei hänen mielestään aina ollut otettu riittävästi huomioon. Vuoden 1998 toimintakertomuksessa (s. 287) myös oikeusasiamies Lauri Lehtimaja oli jo kiinnittänyt huomiota ihmisten perusoikeuksien toteutumisen ja tietoturvallisuuden väliseen suhteeseen (EOA dnro 150/4/98). Lehtimaja totesi, että tietotekniikan lisääntyvä käyttö julkishallinnossa on vaikuttanut myös hallinnon asiakkaiden oikeusasemaan. Laillisuusvalvonnan kannalta on erityisen tärkeätä, että julkishallinnon atk-toiminnot perustuvat selkeisiin ja sitoviin normeihin, että vastuut palvelutuotannossa määritellään ja että julkisuus ja salassapito toteutetaan joustavasti. Tietoverkoissa tarjottavien julkisten palveluiden tulisi olla luotettavia.

Nähdäkseni hallinnon rakennemuutos ja uudentyyppiset organisaatiot sekä atk-alan suositukset ovat osoittautuneet ongelmallisiksi hallinnon perinteisen valvottavuuden ja tarkastettavuuden kannalta. Laillisuusvalvonnan ala kapenee, kun hallintoviranomainen tilaa sopimuspohjaisesti tietojenkäsittely- tai tietoverkkopalveluita atk-palveluyritykseltä. Tämän sopimussuhteen ulkopuolella oleva kansalainen ei yleensä saa korvausta virheistä tai vahingoista ainakaan tältä yritykseltä. Viranomainen voi puolestaan vedota siihen, että se on menetellyt tavanomaisen huolellisesti valitessaan luotettavaa palveluyritystä. Tietoturvallisuutta koskevissa järjestelyissä luotetaan nykyisin erilaisiin tietoturvakartoituksiin, konsultteihin ja sopimuspohjaisiin atk-varakeskuspalveluihin. Liikeyrityksillä on perustuslain 124 §:n säännöksen puitteissa käytännössä merkittävä osuus tietoturvallisuuden ylläpidossa. Mikäli nämä järjestelyt jonkin ennalta arvaamattoman syyn vuoksi pettävät, on julkisen hallinnon asiakas usein käytännössä vailla lain suojaa.

Oikeusasiamiehen näkökulmasta on pidetty tarpeellisena, että atk-palvelusopimusten ja tieto-turvallisuussuositusten rinnalle säädetään erityinen tietoturvallisuuslaki, jolla turvataan perusoikeuksien toteutuminen ja hyvän hallinnon periaate myös muuttuvassa toimintaympäristössä. Nykyiset VAHTI-ohjeet ovat monilukuisuudestaan ja kattavuudestaan

huolimatta tässä säädösteknisessä mielessä nähdäkseni osin ongelmalliset (ks. luonnos s. 8). Samalla voitaisiin laissa selkeästi organisatorisesti määrätä, minkä viranomaisen tehtäväksi tulisi vastata tietoturvallisuuden koordinoinnista. Tällainen viranomainen voi siis nähdäkseni olla hyvinkin valtiovarainministeriö (vrt. jo 22.8.2003 kumottu asetus valtionhallinnon tietohallinnosta 155/1988). Kehittämisohjelman luonnoksessa ei tosin ole selkeästi analysoitu sitä, mikä pakottaa palaamaan tietoturvallisuuden koordinoinnissa varsin keskitettyyn ohjausmalliin (vrt. VTKK/ VIP).

Mielestäni entisten oikeusasiamiesten Lehtimajan ja Paunion tietoturvallisuudesta esittämät ajatukset ovat edelleen ajankohtaisia, sillä informaatio-ohjauskin on nykyisessä resurssipulassa olevassa hallinnossa ajoittain tehotonta (vrt. luonnos s. 8). Tähdennän uudelleen erityisesti sitä, että puutteet julkisissa verkkopalveluissa saattavat vaikuttaa myös kansalaisille tarjottaviin palveluihin ja heidän oikeuksiinsa. Katson myös, että olisi syytä selvittää, millä tavalla yksityiselle korvataan vahingot, jotka aiheutuvat julkishallinnon käyttämien tietojärjestelmien virheistä.

Yksityisten kansalaisten tietotekniikan käyttö ja sähköinen asiointi, virkamiesten esiintyminen sosiaalisessa mediassa sekä ulkoistettujen julkisten verkkosivustojen ja uusien yhteistyömuotojen ylläpidon vastuut (vrt. ENISA Cloud Computing Risk Assessment[1)] ovat kuitenkin kehittämisohjelman yhteydessä mielestäni riittämättömästi selvitetyt.

Tietoturvallisuus on nykyisessä verkottuneessa yhteiskunnassa varsin globaali asia. Siten tietoturva-asioissa harmonisoituva kansainvälinen kehitys ja uusimmat tietoturvallisuussuositukset olisivat ansainneet kehittämisohjelmassa merkittävän osuuden ja aseman mittapuuna[2)].

2) Oikeusasiamiehen kanslian edellytykset ja valmiudet kehittämisohjelman toimeenpanoon

Tietoturvallisuuden kehittäminen edellyttää teknis-/hallinnollisesta näkökulmasta 1) organisaation johdon tietoturvallisuusvastuiden määrittelyä tietoturvallisuusarvioinnissa ja päätöksenteossa 2) tietoturvariskien hallinnan ja riskiarvioinnin kehittämistä 3) tietoturvallisuuden hallintajärjestelmän määrittelyä sekä 4) tietoturvallisuuden pätevyyden, auditoinnin ja jatkuvuuden määrittelyä.

Näiden järjestelyjen sääntely ja sen valvonta julkishallinnossa on myös olennainen osa tietoturvallisuutta ja sen kehittämistä. Kehittämisohjelman luonnoksessa onkin edellytetty, että Valtioneuvoston 26.11.2009

---

1) Kuten tunnettua, tarkoitetaan "pilvipalveluilla" tietotekniikkapalveluiden ulkoistamista verkon yli. Palveluna hankittava infrastruktuuri, sovellusympäristö ja/tai sovellukset sijaitsevat toimittajan palvelimilla ja asiakas ottaa näihin yhteyttä Internetiä käyttämällä.

2) Ks. EU – ENISA, the European Network and Information Security Agency ja sen Digital Agenda-suositukset sekä OECD-periaatteet: OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security 25.7.2002.

tietoturvallisuuden kehittämisestä antaman periaatepäätöksen mukaisesti annetaan asetus tietoturvallisuudesta ja hyvästä tiedonhallintavasta valtionhallinnossa. Asetuksen tavoitteena on luoda edellytykset valtionhallinnon tietoturvatyön kehittämiseksi sekä yhtenäisten menettelyjen luomiseksi tietoaineistoja käsiteltäessä (ks. kehittämisohjelman luonnos s. 13–15).

Tässä yhteydessä on pantava merkille se perustuslain 80 §:n 1 momentin lähtökohta, että asetuksen sijaan lailla on kuitenkin säädettävä yksilön oikeuksien ja velvollisuuksien perusteista sekä asioista, jotka perustuslain mukaan muuten kuuluvat lain alaan. Tässä suhteessa voi nähdäkseni syntyä tulkintatilanteita, kun kansalaisten käyttöön suunnitellaan ja toteutetaan hallinnon asiakkaiden tunnistamisjärjestelmiä ja henkilökohtaisia verkkosivuja sekä kehitetään sisäisen turvallisuuden järjestelmiä[3)].

Laillisuusvalvonta on hallinnon kehitystä seuraavaa ja tarvittaessa hallinnonalat ylittävää valvontatoimintaa. Oikeusasiamiehen näkökulma IT-toimintaan on siten toiminnan laillisuus ja hallinnon asiakkaiden oikeus saada kelvollisesti ja laillisesti palveluita. Näistä lähtökohdista käsin on selvää, että myös virastojen tietojärjestelmillä on vaikutuksia kansalaisten eri perusoikeuksien toteutumiseen. Ensinnäkin kyse on keinosta, jolla turvataan kansalaisten yhdenvertainen kohtelu julkisessa palvelutuotannossa (perustuslain 6 §). Tämän lisäksi on virastojen tietohallinnolla ja –järjestelmillä on ulkoisia vaikutuksia hallintotoiminnan julkisuuteen (perustuslain 10 § 2 mom.) ja asianmukaisuuteen sekä sisäisesti viraston henkilökunnan kohteluun. Molemmissa tapauksissa olisi turvattava oikeus oikeusturvaan ja hyvään hallintoon (perustuslain 21 §). Oikeusasiamiehellä on myös roolinsa hyvän hallinnon kehittäjänä ja varsinkin hallintolain (434/2003) tulkitsijana. Oikeusasiamiehen laillisuusvalvonnassa korostuvat menettelylliseen oikeusturvaan liittyvät kysymykset. Tämä johtuu siitä, että oikeusasiamies ei voi kumota eikä muuttaa tuomioistuinten tai viranomaisten ratkaisuja eikä puuttua niiden harkintavaltansa rajoissa tekemien ratkaisujen lopputuloksiin. Laillisuusvalvonnassa on jouduttu kiinnittämään huomiota muun muassa päätösten joutuisaan käsittelyyn, asianosaisten kuulemiseen, oikeuteen saada palvelua omalla äidinkielellään, asian selvittämiseen, päätösten perustelemiseen sekä huolellisuuteen asian käsittelyssä. Näiden yleisten vaatimusten yhteys sähköiseen hallintoon on hyvinkin läheinen, kun asiointi- ja verkkopalveluihinkin kuuluvat tietopalvelut ja tiedottaminen, asiakaspalaute ja kansalaisten osallistuminen, vireillepano sekä vuorovaikutteiset asiointipalvelut. Julkisten viranomaisten on puolestaan maksimoitava mm. perustuslain 6 §:n puitteissa yhdenvertaisuus ja minimoitava IT-toiminnan käsittelyvirheet.

---

3) Vrt. myös OECD:n tuore Suomea koskeva maa-arviointi 31.5.2010, Internetissä www.vm.fi/vm/fi/03_tiedotteet_ja_puheet/01_tiedotteet/20100531OECDSu/OECD_arviointi.

Oikeusasiamies tutkii siis eduskunnan oikeusasiamiehestä annetun lain (197/2002) lähinnä kansalaisilta saapuvia kanteluita, mutta voi myös oma-aloitteisesti puuttua asioihin ja tehdä esityksiä epäselvän lainsäädännön täsmentämiseksi. Siten oikeusasiamies voi laillisuusvalvontaansa kuuluvassa asiassa tehdä toimivaltaiselle viranomaiselle esityksen tapahtuneen virheen oikaisemiseksi tai epäkohdan korjaamiseksi. Tällainen virhe on voinut käytännössä koskea myös tietoturvallisuutta, kuten jo 1980-luvun alun verohallinnon atk-virheet osoittivat. Edelleen 1990-luvun alussa pohdittiin oikeusasiamiehen kansliassa oikeusasiamiehen mahdollisuuksia suorittaa valvottavien virastojen tarkastusta ja laillisuusvalvontaa tietoverkon kautta.

Lausuntopyynnössä on edellytetty, että kaikki ministeriöt, virastot ja laitokset toteuttavat ja sitoutuvat tietoturvallisuuden kehittämiseen. Eduskunnan oikeusasiamiehen kanslia (noin 60 virkamiestä) on erillisvirastona osa eduskuntaa ja saa pääosin eduskunnan tietohallinnolta tietotekniset palvelunsa (kuten sähköisen työpöydän palvelualustan). Osana eduskunnan tietohallintoa kehitetään myös tietoturvallisuutta. Käytännön yhteistyö valtioneuvoston kanssa on kuitenkin välttämätöntä yhteisen tietoturvallisuudenkin kehittämiseksi. Tietenkin jokaisella organisaatiolla on lakisääteiset velvoitteensa kehittää hyvää tiedonhallintatapaansa ja tietoturvallisuuttaan (ks. kehittämisohjelman luonnos s. 23). Kehittämisen perustana valtionhallinnossa ovat varsinkin julkisuuslaki, henkilötietolaki, laki sähköisestä asioinnista viranomaistoiminnassa, henkilökorttilaki ja arkistolaki.

Nykyinen verkottunut julkishallinto edellyttää myös asiantuntevaa valvontaa ja eri valvontaviranomaisten välistä yhteistyötä. Esimerkkeinä tällaisesta ovat sekä Valtiontalouden tarkastusviraston IT-foorumit (6.11.2008[4] ja 28.1.2010) että Kansallisarkiston kahtena viime vuonna koolle kutsuma arkistointiasioiden yhteistyöverkoston. Oikeusasiamiehen kanslian edustaja on ollut mukana kummassakin yhteistyömuodossa.

3) Kehittämisohjelman hyödyt

Hyvän hallinnon ja siihen liittyvän tietoturvallisuuden kehittäminen on pitkäjänteistä työtä. Se liittyy keskeisiin perustuslain ja yleishallintooikeuden säädöksiin. Perustuslain 21 §:ssä perusoikeutena turvattuun hyvään hallintoon kuuluu osaltaan hallinnon palvelujen tarjoaminen tehokkaasti ja tuloksellisesti. Tietoturvallisuuden kautta turvattavia perusoikeuksia ovat erityisesti perustuslain 10 §:n mukainen yksityiselämän suoja ja perustuslain 12 §:ssä säädetyt sananvapaus ja julkisuus. Sähköisen viestinnän tietosuojalailla (516/2004) oli tavoitteena turvata sähköisen viestinnän luottamuksellisuutta ja yksityisyyden suojan toteutumista. Sillä pyrittiin edistämään myös sähköisen viestinnän tietoturvaa ja

4) Ks. http://www.vtv.fi/ajankohtaista/tiedotearkisto/2008/valtiontalouden_tarkastusviraston_it-foorumi_6.11.2008.html.

monipuolisen sähköisen viestinnän palvelujen tasapainoista kehittymistä. Hallintolain (4345/2003) 7 §:n palveluperiaatteen mukaan asiointi ja asian käsittely viranomaisessa on pyrittävä järjestämään siten, että hallinnossa asioiva saa asianmukaisesti hallinnon palveluita ja viranomainen voi suorittaa tehtävänsä tuloksellisesti. Kehittämisohjelman painotukset, vastuiden selkiyttäminen, tietoturvallisuustiedon lisääminen parantanevat myös hallinnon asiakkaiden oikeusturvaa ja palveluiden laatua.

Näiden peruslähtökohtien huomioon ottaminen sekä hallinnon asiakkaiden aseman ja tietoturvaodotusten selvittäminen olisi kuitenkin kehittämisohjelmassa paikallaan. Paitsi organisatoriset uudistukset olisivat myös kansalaisten luottamuksensuojan ja hallinnon legitimiteetin kannalta tärkeitä atk-virheiden korvaaminen asiakkaille ja ns. nollavirhetoleranssi.

4) Resurssi- ja kustannusvaikutukset

Oikeusasiamiehen kanslia on erillisvirastona mukana eduskunnan tietojärjestelmien kehitystyössä ja eduskunnan tietohallinnon johtoryhmässä. Eduskunnan moniportaisen, verkottuneen ja hajautetun tietohallinnon tarpeisiin nähden tietoturvallisuuden ohjeistusta on jatkuvasti kehitetty siten, että eduskunnan tietojärjestelmistä on suoritettu tietoturvallisuuden arviointeja ja auditointeja sekä annettu ohjeita muun ohella sähköpostin käytöstä. Viime vuosina on eduskunnankin tietohallinnon kehittämistä ja uusia palveluja rajoittanut taloudellinen taantuma. Kuitenkin kehitteillä on mittavia uudistuksia 6.4.2010 käyttöönotetun sähköisen työpöydän lisäksi myös vuosille 2011–2012 suunnittelun sähköisen asianhallinnan osalle. Tässä mielessä on seurattu myös Valtiokonttorin ns. VALDA-hanketta.

5) Osallistuminen yhteistyöhön

Eduskunnan oikeusasiamies on perustuslain 109 §:ssä tarkoitettu valvontaviranomainen. Oikeusasiamiehen toiminnassa suoritetaan projektitarkastuksia ja valitaan vuosittaisia tarkastusteemoja. Tällaisia teemoja ovat olleet muun ohella kansalaisille annettava neuvonta, julkisuuslain toteuttaminen ja hallinnon monikielisyys. Kuten edellä jo totesin, yksittäiset kantelut tuottavat tietoa tietotekniikkapalveluiden systeemivirheistäkin.

Lopuksi tähdennän, että julkishallinnon toimiva ja vastuullisesti järjestetty tietoturvallisuus on nykyisin verkottuneessa hallinnossa välttämätön edellytys kansalaisten ja asiakkaiden perusoikeuksien, kuten julkisuuden ja yksityisyyden suojan, toteutumiselle. Tietoturvallisuus on osa hyvää hallintoa. Tietoturvallisuus on edellytyksenä jo käytössä olevalle verkkotunnistamiselle ja -maksamiselle (VETUMA) sekä kehitteillä oleville kansalaisen verkkosivulle (SADe-hanke) ja kansalaisten asiointitilille. Käy-

tännön tietoturvallisuustoimenpiteillä ja erityisesti hyvillä salauskäytännöillä on olennainen merkitys hallinnon asiakkaille tarjottavissa laajenevissa verkkopalveluissa.

Apulaisoikeusasiamies Jussi Pajuoja

Esittelijäneuvos Jorma Kuopus