Martti Lehto, Jyväskylän yliopisto
4.12.2020

Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä eräiksi siihen liittyviksi laeiksi

Asia: Hallituksen esitys HE 212/2020 vp

1. Digitalisaation mahdollisuudet

Yhteiskunnan yksityiset ja julkiset palvelut perustuvat yhä laajemmin ihmisten, erilaisten toimijoiden ja älykkäiden koneiden ekosysteemin. Kehittyvässä digitaalisessa yhteiskunnassa mahdollisuuksien tila laajenee, jota laajentavat kyberfyysiset toisiinsa kytkeytyneet järjestelmät, vuorovaikutteisuus, itse tuottaminen ja jakaminen, sekä koneiden älykkyyden ja kyvykkyyden kasvu. Digitaalitalouden kehitystä edistävät erilaisten palveluiden ja tietokäytäntöjen digitalisoituminen ja siirtyminen verkkoon. Näin muodostuu digitaalinen alustatalous, jossa elementteinä ovat teollinen internet (Internet of Things, IoT), erilaiset sosiaalisen median ja viestinnän alustat sekä hajautetut yksityiset ja julkiset verkkopalvelut. Tässä digitalisaatioprosessissa hyödynnetään teknologisen kehityksen uusia mahdollisuuksia. Kansalaisten mahdollisuus lisätä hyvinvointitietojaan tai erilaisten hyvinvointisovellusten tuottamia tietoja omatietovarantoon, on osa tätä digitalisaatioprosessia.

Digitalisaation aiheuttaa suuria muutoksia kaikilla liiketoimialoilla. Digitalisaatio on muuttanut perustavalla tavalla yritysten toimintamalleja tuotannosta logistiikka- ja arvoketjujen hallintaan ja markkinointiin. Digitaalinen murros perustuu ihmisten muuttuneisiin odotuksiin, yhteiskunnan palvelurakenteiden ja -tuotannon kasvaneisiin tehokkuusvaatimuksiin ja teknologioiden tarjoamiin mahdollisuuksiin. Uudet teknologiat, työkalut ja toimintatavat muuttavat ihmisten tapaa toimia arjessa ja työssä, organisaatioiden tapaa toteuttaa tehtäviään ja julkishallinnon tapaa tuottaa palveluita eli koko yhteiskunnan toimintalogiikka muuttuu.

SOTE-alan muutoksen tärkeä väline on juuri digitalisaatio. Jatkossa tietojärjestelmät ja uudet sähköiset älykkäät palvelut tukevat asiakkaita ja sosiaali- ja terveydenhuollon ammattilaisia entistä paremmin. Digitalisaation avulla palveluita myös voidaan tuottaa täysin uusilla tavoilla ja tehostaa toimintaprosesseja. Kuten esimerkiksi juuri kansalaisten mahdollisuudella itse ylläpitää toimintakykyään ja terveyttään.

Tulevaisuuden sosiaali- ja terveydenhuollon palvelujärjestelmän toimivuus edellyttää älykkäitä ICT-ratkaisuja, joilla asiakkaiden tietoja voidaan käyttää organisaatio- ja aluerajoista riippumattomasti sekä ensisijaiseen että toissijaiseen käyttöön.

2. Digitalisaation uhat

Haittaohjelmien ja kyberhyökkäysten määrä kasvaa edelleen. Tänä vuonna on tuotettu jo yli 1,2 miljardia haittaohjelmaa. Päivittäin löydetään yli 350 000 uutta haittaohjelmaa ja kun mukaan lasketaan vanhojen haittaohjelmien variantit uusia on vastassamme yli 3 miljoonaa joka päivä.

Raporttien mukaan kyberuhkien merkittävimmät trendit olivat kiristyshaittaohjelmien kasvu, haavoittuvuuksien hyödyntäminen tietojärjestelmissä, fyysisiin laitteisiin kohdistuvat uhkat, yrityksen sisäpiiri hyökkäyskanavana, liiketoiminnan lamauttamiseen tähtäävät hyökkäykset sekä henkilötietojen varastamiseen tähtäävät hyökkäykset.

SOTE-alan tiedoista ovat kiinnostuneet ensisijaisesti rikolliset, mutta myös tiedustelupalvelut ovat kiinnostuneita erityisesti tärkeiden henkilöiden terveystiedoista. Esimerkiksi vuonna 2018 kyberhyökkäyksellä anastettiin 1,5 miljoonan singaporelaisen terveystiedot ml. maan pääministerin Lee Hsien Loongin terveystiedot. Sairaala on myös houkutteleva kohde, niille, jotka haluavat lamauttaa yhteiskunnan elintärkeitä toimintoja.

Tiedustelun siirtyminen verkkoon on tapahtunut samassa tahdissa yhteiskuntien digitalisaation kanssa. Kehittyneimmille vakoiluohjelmille on ollut tyypillistä, että ne on havaittu vasta vuosia operaation alkamisesta. Keskeistä kybertiedustelun kehitykselle on ollut haittaohjelmien monimutkaisuuden ja kyvykkyyden kasvu samalla kun niiden havaitseminen on käynyt yhä vaikeammaksi.

Kyberrikollisuus on monipuolistunut ja se ilmenee yhä laajemmin digitaalisessa toimintaympäristössä. Kyberhyökkäyksillä rikolliset tavoittelevat ensisijaisesti taloudellista hyötyä. Tällaisia ovat mm. identiteettivarkaudet, maksuvälinepetokset, verkkohuijaukset ja -petokset eri muodoissaan jne.

Kyberrikollisuus on merkittävin uhka digitaalisessa kybermaailmassa. Yli 80 % hyökkäyksistä on edelleen taloudellisesti motivoituneita. Menetyksistä kyberrikollisuudelle esitetään erilaisia arvioita, mutta ne ovat vuosittain luokkaa 6 biljoonan (6000 miljardia) dollaria ja kasvuvauhti on 15% vuodessa. Menetykset ovat paljon suurempia kuin vuosittaiset luonnonnettomuuksien aiheuttamat kustannukset. Menetykset kyberrikollisuudesta ovat noin 0,5–2,5 % BKT:stä.

Miksi em. tavalla pääsee tapahtumaan? Koska hyökkääjät käyttävät hyväkseen haavoittuvuuksia. Niitä esiintyy ihmisten toiminnassa, organisaatioiden prosesseissa ja käytetyssä teknologiassa. Kovin usein ihminen on heikoin lenkki. Siksi 2/3 hyökkäyksistä perustuu sosiaaliseen manipulointiin (tietojen kalastelu eri muodoissaan, korruptoidut yrityssähköpostit jne.).

Loput 1/3 perustuvat organisaation puutteellisiin kyberturvallisuusprosesseihin kuten salasanakäytänteet, pääsynhallinta, epäselvät toimintaprosessit sekä käytetyn teknologian puutteisiin (ohjelmistovirheet (SW), laitteistovirheet (HW), algoritmi- ja konfigurointi heikkoudet jne.)

3. Kyberturvallisuutta rakentamassa

Kun kerran Ihmiset-Prosessit-Teknologia muodostavat haavoittuvuusympäristön, tulee kyberturvallisuuden rakentua noille kolmelle alueelle.

Henkilöstön osalta kysymys on kyberosaamisen hallinnasta, prosessien osalta organisaation kyberturvallisuus- ja toimintaprosesseista ja teknologian osalta oikein valituista ja toteutetuista teknisistä kyberturvallisuusratkaisuista.

Organisaation kyberturvallisuuden rakentaminen perustuu riittävään osaamiseen. Johdolla on vastuu kyberosaamisen hallinnasta koko henkilöstön osalta. Johdon vastuulla on myös organisaation kyberkulttuuri, jossa jokainen noudattaa toimintaohjeita ja tervettä järkeä.

Organisaation kyberturvallisuus pysyy tai kaatuu valvontaan. Organisaatiossa voidaan laatia kyberturvallisuusohjeet, kouluttaa henkilöstöä, laatia toimivat prosessit ja valita optimaaliset kyberturvallisuusratkaisut, mutta ilman jatkuvaa valvontaa järjestelmä ei pysy kauaa resilienttinä kyberhyökkäyksiä vastaan. Ilman tehokasta organisaation ICT-ympäristön valvontaa organisaatio ei selviydy nykyisessä uhkaympäristössä. Tietoverkkojen valvonta voi olla itse toteutettua tai ulkoistettua.

4. Uuden lain vaikutuksista

4.1 Tavoite

Lakiin ehdotettavien muutosten tavoitteena on luoda edellytykset valtakunnallisten tietojärjestelmäpalvelujen käyttöönotolle sosiaalihuollossa asettamalla sosiaalihuollon palvelunantajille velvoitteen liittyä valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi sekä mahdollistamalla tietojen luovutuksen sosiaalihuollon asiakastiedon arkistosta. Lisäksi esityksessä ehdotetaan valtakunnallisten tietojärjestelmäpalvelujen sisällön laajentamista siten, että asiakas itse voisi tallentaa omia hyvinvointitietojaan tai erilaisten hyvinvointisovellusten tuottamia tietoja omatietovarantoon.

Tällä valtakunnallisten tietojärjestelmäpalveluiden keskittämisellä (Kanta-palvelut, sosiaali- ja terveydenhuollon asiakastiedot, hyvinvointitiedot sekä lääkitystiedot) luodaan valtakunnallinen asiakastietovaranto SOTE-alan palveluntarjoajien asiakastyöhön. Tätä digitalisaatiokehitystä on pidettävä myönteisenä, millä parannetaan kansalaisten sosiaali- ja terveydenhuollon vaikuttavuutta.

Kansalaisten osallistuminen terveydestään ja hyvinvoinnistaan huolehtimiseen parantaa ymmärtämystä hoidosta ja palveluista.

4.2 Järjestelmätason kyberturvallisuus

Kuten lain yleisperusteluissa todetaan arkaluonteisten ja salassa pidettävien tietojen käsittely tietojärjestelmissä edellyttää, että kaikki osapuolet voivat luottaa siihen, että käytettävät teknisesti monimutkaiset tietojärjestelmäkokonaisuudet ovat periaatteiltaan, teknisiltä ratkaisuiltaan ja toteutukseltaan lainsäädännön mukaisia ja täyttävät kaikki tietoturvallisuuden vaatimukset.

Erityisesti potilastietojärjestelmien osalta on erityisen tärkeää varmistua, että kyberturvallisuus on toteutettu asianmukaisesti heti järjestelmän käyttöönoton alkaessa. Tämä edellyttää, että kyberturvallisuus on otettu huomioon laitteiden ja järjestelmien suunnitteluvaiheesta alkaen (Cyber Security by Design).

Kansalaisella luodaan mahdollisuus päästä Kanta-järjestelmään käyttäen suojattua kansalaisen käyttöliittymän avulla. Kyberturvallisuuden vahvistamiseksi Kanta-järjestelmään kirjautuminen tulee tehdä vahvan kaksivaiheisen tunnistautumisen kautta.

Hyvinvointisovelluksille tulee luoda esityksen mukaisesti kattava sertifiointimenettely valtakunnallisten tietojärjestelmäpalveluiden liittymisen ehdoksi.

4.3 Kyberturvallisuustoimenpiteiden valvonta

Tiedonhallintalaki sisältää viranomaistoiminnalle yhtenäiset tietoturvallisuuden perusvaatimukset ja lain tavoitteena on varmistaa, että kaikki tiedonhallintayksiköt täyttävät vähintään samat perustason vaatimukset. Lain mukaan tiedonhallintayksikössä on järjestettävä riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta, mikä edellyttää omavalvontaa.

Sosiaali- ja terveydenhuollon toimintayksiköille on säädetty velvollisuus laatia omavalvontasuunnitelma. Oikein toteutettuna tietojärjestelmien omavalvontasuunnitelman avulla voidaan tehostaa organisaation kyberturvallisuutta. Mutta omavalvontasuunnitelma ei ole riittävä, vaan SOTE-toimijoilta, joilla potilastietoja sisältäviä tietojärjestelmiä, tulee vaatia ulkopuolisen toimijan tekemä tietoturva-auditointi ennen järjestelmän käyttöönottoa. Hyväksytyn auditoinnin perusteella myönnetty lupa olisi voimassa kolme (3) vuotta, jonka jälkeen se olisi uusittava. Auditoinnin yhteydessä esiin tulleiden puutteiden vakavuus määrittää korjaustoimenpiteiden aikataulun, ääritapauksessa potilaistietojärjestelmän käyttö on keskeytettävä välittömästi. Valviran tehtävä olisi johtaa järjestelmien sertifiointia ja auditointia, ja käytännön toimintaa tekisivät auktorisoidut sertifiointi- ja auditointilaitokset.

Auditoinnin ja sertifioinnin avulla edistetään ja vahvistetaan viranomaisten, SOTE-toimijoiden ja kansalaisten keskinäistä luottamusta, mikä on välttämätön edellytys SOTE-järjestelmän toiminnalle, ilman luottamusta järjestelmä ei toimi.

Ehdotuksen mukaan SOTE-tietoja saisi käsitellä käyttötarkoituksen mukaisessa laajuudessa. Käyttöoikeushallinnalla, henkilöstön kouluttamisella sekä teknisillä ja organisatorisilla toimenpiteillä pyritään estämään tietojen oikeudeton käyttö. Lisäksi käytettävät laitteet ja toimijat on tunnistettava luotettavasti. Lisäksi käyttö- ja luovutuslokitietojen keräämisellä ja lokivalvonnalla varmistettaisiin, ettei väärinkäytöksiä tapahtuisi. Näitä menettelyjä eri organisaatioissa on kyettävä valvomaan.

Ehdotuksen mukaan SOTE-alalla käytettävä tietojärjestelmien sertifiointimekanismi säilyy myös asiakastietolakia uudistettaessa laajentuen sosiaalihuoltoon. Ehdotuksessa esitetty tekniikan kehityksen seuranta ei yksin riitä, tarvitaan selkeä toimintatapamalli, jolla varmistetaan uhka- ja riskiympäristöön oikein suhteutetun kyberturvallisuusteknologian käyttö SOTE-tietojärjestelmissä.

Erityisen tarpeellista on ehdotuksessa mainittu vaatimus siitä, että Kelalle lisättäisiin oikeus toteuttaa tietojärjestelmiensä ja niihin sisältyvien tietojen käytön valvontaa niin, että sillä olisi nykyistä parempi mahdollisuus tunnistaa poikkeavaa toimintaa. Siksi havainnointi tulee ulottaa tieto- ja informaatiovirtoihin ulkoa organisaation sisään ja sisältä ulos ja prosesseihin organisaation sisällä. Vain tehokkaalla järjestelmien ja käytön valvonnalla voidaan kyberuhkia tunnistaa riittävän tehokkaasti.

Esityksessä esitetään, että valtakunnallisten tietojärjestelmäpalvelujen yhteyteen perustettaisiin omatietovaranto, jonne henkilöt voivat tallentaa omia hyvinvointitietojaan. Henkilö voisi päättää omatietovarannossa olevien hyvinvointitietojensa tai hyvinvointisovellusten tuottamien tietojen käytöstä. Laajan käyttäjäjoukon tietovarannon hallinta vaatii erityisen tehokkaat kyberturvallisuustoimenpiteet.

SOTE-alan tietojenkäsittelyn vaatimusten tulee perustua kyberturvallisuutta koskeviin vähimmäisvaatimuksiin sekä riskiperusteiseen arviointiin ja siihen perustuvaan kyberturvallisuustoimenpiteiden toimeenpanoon.

SOTE-tietojärjestelmien auditoinnin ja valvonnan osalta voidaan soveltaa suhteellisuusperiaatetta, joka mahdollistaa eri toimijoiden erityispiirteiden ottamisen huomioon. Suhteellisuusperiaatteen käytössä on olennaista arvioida toimijan vaikutusta koko SOTE-yhteisöön, eikä yksinomaan sen kokoa. Laajavaikutteinen kyberhäiriötilanne voi lähteä liikkeelle myös pienen toimijan kyberturvallisuustoimenpiteiden laiminlyönnistä.

4.4 SOTE-alan kyberturvallisuuden tilannekuvan vahvistaminen

Nykyisen tietosuoja-asetuksen mukaan rekisterinpitäjän on ilmoitettava tietosuojavaltuutetulle henkilötietojen tietoturvaloukkauksesta, jos siitä voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille.

SOTE-alan kyberuhkaympäristön paheneminen edellyttää SOTE-alan kyberturvallisuustoimijoiden luottamusverkoston vahvistamista. Samalla tulee kybertapahtumien ilmoitusvelvollisuutta entisestään laajentaa parantamaan kyberuhkatietoisuutta. Toimijoiden tulisi raportoida laajoista ja myös pienistä kyberturvallisuustapahtumista, sillä pienetkin tapahtumat tuovat esiin ns. hiljaisia signaaleita, joita tarvitaan kattavaan tilanneymmärrykseen.

Kaikkinaista SOTE-toimijoiden välistä vapaaehtoispohjalta tapahtuvaa kyberuhkia koskevaa tietojenvaihtoa tulee edistää. Tietoisuuden lisääminen kybermaailman tapahtumista ja ilmiöistä vahvistaa jokaisen organisaation kyvykkyyttä oman kyberriskienhallintansa kehittämisessä.

SOTE-ala ja ICT-palveluiden tuottajat muodostavat toisiinsa linkittyneen keskinäisriippuvan verkoston ja useissa tapauksissa tunkeutuminen organisaation tietojärjestelmään on tapahtunutkin kolmannen osapuolen kautta. Siksi jokaisella SOTE-organisaatiolla tulee olla riittävä kyky havainnoida kaikkia informaatiovirtoja ja toimintaprosesseja, jotta kaikki epänormaalitoiminta voidaan havaita. Havainnointikyky luo perustaa oikeinmitoitetuille kyberturvallisuustoimenpiteille ja varautumiselle.

4.5 Kyberturvallisuusosaamisen ja -tutkimuksen vahvistaminen

Lakiluonnos kuvaa prosesseja ja teknologian kehittämisperiaatteita luotaessa sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä. Lakiluonnos ei ota kantaa tarvittavaan kyberturvallisuusosaamisen parantamiseen kaikkien SOTE-toimijoiden piirissä. Kuten edellä on todettu ihmisten aiheuttavat riskit ovat merkittäviä organisaation kyberriskien hallinnassa. Osaamisenhallinnan varaan rakentuu organisaation kyberturvallisuuden rakentaminen.

Tässä yhteydessä tulee painottaa kyberturvallisuusosaamisen vahvistamista kaikkien SOTE-alan toimijoiden keskuudessa. Tarvitaan kyberosaamista kansalaistaidoista aina huipputason erityisosaamiseen, jotta voidaan aikaan saada kansallisen tason kyberresilienssiä eri kyberuhkatilanteisiin.

Tarvitaan laaja SOTE-alaa käsittävä tutkimus eri toimijoiden käytössä olevien tietojärjestelmien nykytilasta suhteessa vallitsevaan kyberturvallisuustilanteeseen. Toisena tutkimusalueena olisi uuden lain mukanaan

tuomien toimenpiteiden implementoinnin edellyttämät täsmälliset toimenpiteet ja vaikuttavuusanalyysin laatiminen.

4.6 Lain täytäntöönpanoon tarvittavien resurssien osoittaminen

Kuten esityksessä todetaan, ehdotuksella on välittömiä taloudellisia vaikutuksia sekä valtiontalouteen että sosiaali- ja terveydenhuollon palveluntarjoajille ja apteekeille. Ehdotuksessa on kuvattu tarvittavia lain toimeenpanon edellyttämiä kustannuksia julkishallinnossa.

Ehdotuksessa lueteltuihin keskeisin rahoitustarvetta edellyttäviin kehittämiskohteisiin tulee lisätä kyberturvallisuuden vahvistamisesta aiheutuvat kustannukset. Tarvitaan investointeja laitteisiin ja tietojärjestelmiin, kybertilannekuvan luomiseen eri organisaatioissa, auditointi- ja sertifiointiprosessien vahvistamiseen, kyberosaamisen tehostamiseen sekä SOTE-alan kyberturvallisuuden tutkimukseen.

Kustannuksia aiheutuu myös yksityisen sektorin toimijoille kyberturvallisuutta rakennettaessa. SOTE-alan on yksi merkittävä osa yhteiskunnan kriittistä infrastruktuuria ja elintärkeitä toimintoja, jonka toiminta normaaliaikojen häiriötilanteissa ja poikkeusoloissa tulee turvata julkisen sektorin vahvalla tuella. Siksi julkisen sektorin tulee luoda tukimekanismeja myös yksityisen sektorin toimijoille, jotta SOTE-alalle kokonaisuudessaan voisi kehittyä kyberturvallinen toimintaympäristö.

Kaikkien toimijoiden tulisi nähdä kyberturvallisuus toiminnan varmistajana ja toimintaedellytysten luojana, eikä kustannuseränä.

Tutkimus vuosilta 2017–2018 kertoo, että kyberhyökkäyksen jälkeiset toiminnan palautus- ja korjauskustannukset ovat keskimäärin 1,1 miljoonaa dollaria yritystä kohden ja SOTE-alalla kustannukset ovat korkeammat - 1,4 miljoonaa dollaria. Näillä summilla olisi rakennettu paljon hyvää kyberturvallisuutta.

Työelämäprofessori, ST Martti Lehto
Jyväskylän yliopisto, Informaatioteknologian tiedekunta
martti.lehto@jyu.fi