

Sosiaali- ja terveysvaliokunta

KYBERTURVALLISUUDEN MERKITYS SOSIAALI-JA TERVEYSTIEDOISSA

Teknologisen kehityksen ja digitalisaation syventyessä digitaalisen toimintaympäristön turvallisuuden, kyberturvallisuuden, merkitys korostuu. Kyse on olennaisesti luottamuksen säilymisestä digitalisaation ja teknologian kehityksen myönteisiin kehityspiirteisiin. Samassa yhteydessä voidaan puhua ”räjähdysmäisestä” datan ja tiedon määrän kasvusta maailmassa, kun erilaista dataa ja tietoa kerätään yhä moninaisemmin ja tehokkaammin. Tiedon omistajuus, turvallisuus ja ylipäänsä tiedon hyväksikäyttämiseen liittyvät kysymykset nousevat yhä merkityksellisemmiksi. Suomi on yksi maailman digitalisoituneimmista yhteiskunnista.

Tiedon turvaamisen yhteydessä puhutaan yleensä tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta. Luottamuksellisuudella tarkoitetaan, että organisaation tehtäviin liittyvät turvallisuusluokitellut, muutoin salassa pidettävät ja arkaluonteisia henkilötietoja sisältävät asiakirjalliset tiedot ovat vain niiden käytettävissä, joilla on käyttöoikeudet kyseisiin tietoihin. Saatavuus tarkoittaa sitä, että asiakirjallisten tietojen tulee olla helposti ja viiveettä niiden käytössä, joille tieto kuuluu. Samalla on huolehdittava, että asiakirjalliset tiedot saadaan teknisesti esille. Eheydellä puolestaan tarkoitetaan sitä, että asiakirjalliset tiedot ovat oikeita ja ajan tasalla, asiakirjalliset tiedot eivät saa muuttua, hävitä eivätkä vahingoittua virheiden/luvottomien toimenpiteiden seurauksena.

Viime aikoina yhä enemmän kansainvälisissä tutkijapiirissä on korostunut tiedon eheydestä huolehtimisen merkitys. Kyse on pelkistäen siitä, että tiedon ja datan oikeellisuuteen voidaan luottaa. Esimerkiksi potilastiedoissa on oltava varmuus siitä, että tiedot ovat oikein ja että ne ovat muuttumattomat (ja säilyvät muuttumattomina). On huomioitava, että esimerkiksi Yhdysvalloissa turvallisuusviranomaiset ovat nostaneet datamanipulaation yhdeksi keskeiseksi yhteiskunnalliseksi uhkakuvaksi. Jatkossa suurin ongelma ei välttämättä ole se, että data/tieto menetetään tai että se tuhoutuu, vaan että tiedon eheys muuttuu tarkoituksellisen datamanipulaation tai tahattoman toiminnan tuloksena.

Kyberturvallisuuden näkökulmasta on tiedon turvaamisessa ymmärrettävä alati muuttuvaa uhkakenttää ja eri toimijoita. Rikolliset ovat sellaisen tiedon perässä, josta on saatavissa rahallista arvoa. Esimerkiksi ihmisten terveystiedot ovat internetin pimeillä markkinoilla ”kuumaa tavaraa.” Toisaalta viime vuosina yleistyneet kiristyshaittaohjelmat ovat erityisen haitallisia terveydenhuoltoalalle, sillä esimerkiksi mikäli pääsy potilastietojärjestelmiin estyy kiristyshaittaohjelman takia, voivat seuraukset olla hyvinkin vakavia. Valtioille kybertoimintaympäristöstä on tullut strateginen ympäristö, jossa eri tavoin pyritään edistämään valtiollisia poliittisia tavoitteita. Tämän päivän hybridivaikuttamisessa pyritään nimenomaan horjuttamaan yhteiskunnan rauhaa ja vakautta, ja vaikuttamisen keskeisenä kohteena ovat yhteiskunnan kansalaiset sekä heidän luottamuksensa yhteiskunnan toimintaan. Tässä yhteydessä vaikuttaminen digitaalisiin terveystietojärjestelmiin sekä digitaalisiin terveystietoihin nousee merkittäväksi yhteiskunnalliseksi uhkatekijäksi. Valtioneuvoston kanslialle vuonna 2017 tehdyssä

”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” -tutkimuksessa nostettiin juuri terveydenhuoltoala erityiseksi vaikuttamisen kohteeksi tulevaisuudessa Suomen kyberturvallisuudessa.

On tärkeää, että kaikessa suomalaisen yhteiskunnan digitaalisen tiedon turvaamisessa kyetään jatkuvaan ymmärrykseen eri uhkatekijöiden toimintatapojen kehityksestä, että tiedon turvaamisen muuttuvista sekä kehittyvistä tavoista. Laaja poikkihallinnollinen ja -yhteiskunnallinen yhteistyö sekä myös kansainvälinen yhteistyö on välttämättömyys. Kaiken kaikkiaan kyse on tietoturvallisuuden jatkuvasta ja aktiivisesta kehittämisestä niin ratkaisuiden, toimintatapojen kuin osaamisen kehittämisen osalta.

Suomalaisen digitaalisen yhteiskunnan tietovarantojen turvallisuudesta (luottamuksellisuus, eheys ja saatavuus) huolehtiminen on koko yhteiskunnan vakauden ja turvallisuuden näkökulmasta yhä merkittävämpi asia. Erityinen huomio on kiinnitettävä henkilötietojen turvaamiseen ja tiedon oikeellisuuden/eheyden säilymiseen. Tietoturvallisuudesta huolehtiminen edellyttää lähtökohtaisesti turvallisuuden huomioimista kaikessa toiminnassa ja toiminnan tasoilla. Tämän takia on erittäin merkityksellistä, että on määritelty selkeästi tietoturvallisuuden osoittamisen vaatimukset sekä noudatettavat menettelyt. Arviointilaitoksen määrittely on tässä yhteydessä tärkeässä roolissa Hallituksen esityksessä. On myös tärkeää, että valvontaviranomaisilla on mahdollisuus tehdä tarkastuksia tietoturvallisuuden tason konkreettiseksi toteamiseksi ja sen kehittämiseksi.

Aalto-yliopisto

Professori

Jarno Limnéll