

Hallintovaliokunta
HaV@eduskunta.fi**Liikenne- ja viestintäministeriön lausunto valtioneuvoston selonteosta sisäisestä turvallisuudesta (VNS 5/2016 vp)**

Liikenne- ja viestintäministeriön hallinnonalan tavoitteena on mahdollistaa turvaliset ja toimivat liikenne- ja viestintäyhteydet ja -palvelut kestäväällä tavalla kasvun ja uusien digitaalisten palveluiden syntymisen tukemiseksi.

Liikenne- ja viestintäministeriö kiinnittää huomiota siihen, että digitalisaatio nähdään hallitusohjelmassa globaalina megatrendinä ja maan kilpailukyvyyn kannalta tärkeänä mahdollisuutena, jonka hyödyntämiseen Suomella on hyvät edellytykset. Hallitusohjelmalla tavoitellaan tuottavuusloikkaa niin julkisissa palveluissa kuin yksityisellä sektorillakin tarttumalla digitalisaation mahdollisuuksiin ja purkamalla turhaa sääntelyä ja byrokratiaa.

Selonteossa on kuvattu eräitä digitalisaatioon liittyviä uhkia ja mahdollisuuksia. Uusia toimintatapoja tulee kehittää siten, että niihin liittyviä riskejä voidaan tehokkaasti hallita. Liikenne- ja viestintäministeriön hallinnonalalla uuden teknologian, digitalisaation ja uusien liiketoimintakonseptien käyttöönottoa edistettäessä arvioidaan kattavasti niihin liittyviä mahdollisuuksia ja riskejä.

Liikenne- ja viestintäministeriö pitää tärkeänä selonteossa esitettyä huomiota siitä, että ihmisten kokema luottamus viranomaisiin ja toisiaan kohtaan on edellytys turvallisuudelle, turvallisuuden tunteelle ja hyvin toimivalle yhteiskunnalle. Kuten selonteossa on esitetty, turvallisuus on myös merkittävä kilpailutekijä, kun yritykset päättävät maantieteellisestä sijoittumisestaan.

Kuten selonteossa on edelleen todettu, yhteiskunnan arvoilla, kuten perusoikeuksien kunnioittamisella on keskeinen rooli turvallisuuden luomisessa. Liikenne- ja viestintäministeriö yhtyy tähän huomioon ja painottaa eduskunnan aiemmin esittämän ponnen mukaisesti, että palvelujen käyttäjien oikeuksien, kuten yksityisyyden suojan ja luottamuksellisen viestin suojan säilymisestä sähköisissä palveluissa ja verkkoympäristössä on huolehdittava kaikin keinoin (EV 106/2014 vp - HE 221/2013 vp). Tämä tulisi huomioida tulevaisuudessa myös sisäisen turvallisuuden kehittämistyössä, jotta suomalaisten kokema luottamus viranomaisiin ja yrityksiä kohtaan pysyisi korkeana.

Ulkomaisten esimerkkien valossa verkkotiedusteluvaltuuksilla on merkitystä kansalaisten ja yritysten kokemaan luottamukseen ja vaikutuksia yritysten sijoittautumista koskeviin arvioihin. Suomessa lainsäädäntö turvaa jo nykyisin verrattain korkeatasoisen tietosuojan ja tietoturvan tason. Lainsäädäntömme muodostaa yritystoiminnalle kilpailuedun muun muassa niihin valtioihin nähden, joissa viran-

omaisilla on laajemmat oikeudet puuttua yksityiselämän ja viestinnän luottamuksellisuuden suojaan tietoverkoissa ja -järjestelmissä. Kilpailuedun säilyttäminen tulee huomioida myös sisäisen turvallisuuden kehittämistyössä.

Selonteossa on mainittu, ettei siinä kattavasti käsitellä digitalisaatiota, kyberturvallisuutta tai liikenneturvallisuutta, vaan työtä on tarkoitus jatkaa tehtäväksi osana sisäisen turvallisuuden strategian laadintaa. Liikenne- ja viestintäministeriön hallinnonalan toimet tukevat osaltaan myös tätä jatkotyötä.

Hallitusohjelman kärkihankkeen mukaisesti hyväksytyllä Suomen tietoturvasuosisstrategialla pyritään lisäämään digitaalisia palveluita kohtaan koettua luottamusta muun muassa puuttumalla luottamusta heikentäviin ilmiöihin kuten esimerkiksi laajamittaisiin yksityisyyden loukkauksiin ja tietoturvaloukkauksiin. Strategian tavoitteet sekä niitä tukevat toimenpiteet antavat hyvän kuvan siitä, millaisiin toimiin tietoturvasuuden edistämiseksi olisi jatkossa ryhdyttävä.

Korkea tietoturvan taso on edellytys tulevaisuuden yhteiskunnan turvallisuudelle. Kun yhteiskunnan perustavan laatuiset toiminnot digitalisoituvat, on tärkeää, että kansalaiset voivat luottaa niiden turvalliseen toimintaan. Vakavat tietoturvaloukkaukset voivat pahimmillaan uhata yhteiskunnan elintärkeiden toimintojen jatkuvuutta. Liikenne- ja viestintäministeriössä on käynnistynyt säädöshanke, jolla saatetaan kansallisesti voimaan elokuussa voimaan tullut EU:n verkko- ja tietoturvadirektiivi. Direktiivillä velvoittaa jäsenvaltiot ryhtymään toimiin tietoturvariskien hallitsemiseksi useilla eri toimialoilla.

Arkipäiväisten palveluiden edelleen digitalisoituessa, myös tavallisten kansalaisten riski joutua tieto- ja viestintärikollisuuden uhriksi voi kasvaa. Tietoturvasuus ja kyky välttyä tietoverkkorikollisuudelta ovatkin tärkeitä edellytyksiä nykyaikaisten arjen palveluiden turvallisuudelle. Tulevaisuudessa on tärkeää edistää sitä, että markkinoilla tarjoilla olevissa hyödykkeissä ja palvelumalleissa tietoturva on sisäänrakennettua, helppokäyttöistä ja turvaa perusoikeuksien toteutumisen. Viranomaisien tulee myös auttaa yhteisöjä ja kansalaisia tietoturvan parantamisessa.

Tietojärjestelmiä voi olla vaikeaa tai mahdotonta rakentaa niin, että ne olisivat täysin tietoturvasuusia. Yksi keino torjua edelleen tietoturvaloukkauksien aiheuttamia vahinkoja, on huolehtia siitä, että verkko- ja tietojärjestelmissä kulkeva tieto on salattua tai suojattua. Yritykset ovat velvollisia huolehtimaan järjestelmiensä turvallisuudessa esimerkiksi henkilötietojen suojaamiseksi. Selonteossa on todettu, että tietojärjestelmien kasvava salaus on kasvattanut henkilö- ja tietoteknisten poliisin resurssien tarvetta entisestään. Liikenne- ja viestintäministeriö korostaa, että toisaalta tietojärjestelmien tekniset salaus- ja suojausmenetelmät ovat keino vähentää tietoturvaloukkauksista aiheutuvia haitallisia seurauksia ja verkkorikollisuuden uhriksi joutumista.

Liikenteen turvallisuus on keskeinen osa sisäistä turvallisuutta. Digitalisaatio muuttaa myös liikenneturvallisuutta merkittävällä tavalla. Tutkimusten mukaan ihmilliset syyt ovat osasyynä jopa 90 prosentissa liikenneonnettomuuksista. Ajo-
neuvojen automatisoitumisella uskotaan voitavan vähentää ihmillisiä virheitä. Liikenteeseen liittyvien automaattitoimintojen tarvitsema monimuotoinen tieto, tiedon riittävä määrä ja tiedon luotettavuus sekä tiedonvälityksen turvallisuus ovat avainasemassa varmistettaessa älykkäiden liikennejärjestelmien ja automaattisesti ohjautuvien liikennevälineiden turvallisuus.

Liikenteen automaation yleistymisen kannalta on erittäin tärkeää, että kansalaiset voivat luottaa uusiin teknologioihin. Tietoturvallisuus sekä tieto- ja viestintärikosten riskit tulee huomioida liikennejärjestelmää ja liikennepalveluja suunniteltaessa, kehitettäessä ja ylläpidettäessä. Tämä on tärkeää, jotta tieliikenteen ohjaukseen liittyvät ohjelmistot olisivat laadukkaita ja kestäisivät niin tahallisesti kuin tahattomastikin aiheutuvat tietoturvahäiriöt.

Digitalisaatiota voidaan hyödyntää myös liikennesääntöjen ja sanktiojärjestelmän yleisestävän vaikutuksen ja erityisesti kiinnijäämisriskin tehostamiseen. Liikenneturvallisuuden kannalta olisi tärkeää, että poliisin liikennevalvontaa ylläpidettäisiin ja kehitettäisiin liikenneturvallisuutta vaarantavien tekojen estämiseksi. Esimerkiksi automaattista liikenteen valvontaa voisi teknisesti olla mahdollista käyttää kustannustehokkaalla tavalla ylinopeuksien ohella muidenkin liikennetrikomusten ennalta ehkäisemiseen.

Liikenne- ja viestintäministeriö suhtautuu positiivisesti siihen, että tiedonannossa on huomioitu uusien teknologisten innovaatioiden tuomat mahdollisuudet myös sisäisen turvallisuuden lisäämisessä. Liikenne- ja viestintäministeriössä valmistellaan parhaillaan valtioneuvoston periaatepäätöstä liikenneturvallisuuden parantamiseksi. Valmistelu on tehty tiiviissä yhteistyössä muiden ministeriöiden kanssa ja valmistelun yhteydessä nousi esimerkiksi esille, että rattijuopumusvalvonnan kehittämistä huumausaineiden ja lääkkeiden osalta voitaisiin arvioida käynnissä olevan sisäisen turvallisuuden strategiayön yhteydessä.

Lisäksi liikenne- ja viestintäministeriössä valmistellaan kokonaisuudistusta tieliikennelakiin. Näillä ministeriön hankkeilla parannetaan liikenneturvallisuutta sekä poistetaan osaltaan esteitä sille, että liikenneturvallisuutta voitaisiin kehittää uutta teknologiaa ja digitalisaatiota hyödyntäen.

Maija Rönkä
Ylitarkastaja