Anu Mutanen, OTT, apulaisprofessori 24.9.2024

LAUSUNTO EDUSKUNNAN PERUSTUSLAKIVALIOKUNNALLE HALLITUKSEN ESITYKSESTÄ EDUSKUNNALLE KYBERTURVALLISUUSDIREKTIIVIN (NIS 2 -DIREKTIIVI) TÄYTÄNTÖÖNPANOA KOSKEVAKSI LAINSÄÄDÄNNÖKSI (HE 57/2024 VP)

Eduskunnan perustuslakivaliokunnan pyytämänä lausuntona otsikossa mainitusta hallituksen esityksestä esitän kunnioittavasti seuraavan.

Yleistä esityksestä

Hallituksen esityksessä on kyse EU:n kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanosta. Tässä tarkoituksessa säädettäisiin uutena lakina kyberturvallisuuslaki ja tehtäisiin muutoksia useisiin voimassa oleviin lakeihin, kuten julkisen hallinnon tiedonhallinnasta annettuun lakiin ja sähköisen viestinnän palveluista annettuun lakiin. Lait on tarkoitettu tulemaan voimaan 18.10.2024.

Kyberturvallisuusdirektiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta kriittisiksi katsottujen sektoreiden ja toimijoiden osalta velvoittamalla jäsenvaltiot asettamaan direktiivin soveltamisalaan kuuluville toimijoille velvoittavia riskienhallintatoimia kyberturvallisuushäiriöiden varalta.

Esitys sisältää jakson lakiehdotusten suhteesta perustuslakiin ja säätämisjärjestykseen. Jaksossa on viitattu tai tarkasteltu ehdotetun sääntelyn suhdetta perustuslain 2 §:n 3 momentissa säädettyyn julkisen vallan käytön lakisidonnaisuuteen, 8 §:n mukaiseen rikosoikeudellisen laillisuusperiaatteeseen, 10 §:ssä turvattuun yksityiselämän, henkilötietojen ja luottamuksellisen viestinnän suojaan, 12 §:n 2 momentin mukaiseen julkisuusperiaatteeseen, 15 §:ssä turvattuun omaisuudensuojaan, 18 §:n mukaiseen elinkeinovapauteen, 21 §:ssä säädettyyn oikeusturvaan, 80 §:ssä asetuksen antamisesta ja lainsäädäntövallan siirtämisestä säädettyyn, 119 § 2 momenttiin valtionhallinnon toimielinten yleisten perusteiden lakisääteisyyteen sekä 124 §:ssä hallintotehtävän antamisesta muulle kuin viranomaiselle säädettyyn. Asiakysymyksinä on tarkasteltu luottamuksellisen viestinnän suojaa (sähköisen viestin välitystiedot, haitallisen tietokoneohjelman tai käskyn sisältävä viesti, vapaaehtoiset kyberturvallisuustietojen jakamisjärjestelyt, valvovan viranomaisen tiedonsaantioikeus, haavoittuvuuskartoitus), julkisen hallintotehtävän antamista muulle kuin viranomaiselle (ulkopuolisen asiantuntijan käyttäminen apuna tarkastuksessa), elinkeinonvapautta (toimijoiden ilmoittautumisvelvollisuus valvovalle viranomaiselle, luvanvaraisen toiminnan rajoittaminen, johdon toiminnan rajoittaminen), omaisuudensuojaa, hallinnollista seuraamusmaksua, valtion toimielinten yleisiä perusteita, lainsäädäntövallan siirtämistä (valtioneuvoston asetus soveltamisalaan kuuluvien toimijoiden määrittämisestä, määräyksenantovaltuudet), julkisuusperiaatetta, eräiden valtioelinten ja viranomaisten asemaa sekä Ahvenanmaan asemaa ja suhdetta itsehallintoon. Esityksen mukaan lakiehdotukset voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä.

Esityksen perustuslakijakso on varsin kattava ja perusteiltaan pääosin asianmukainen. Arvioissa on otettu huomioon asiassa olennaista perustuslakivaliokunnan tulkintakäytäntöä samoin kuin ihmisoikeuksia koskevaa oikeuskäytäntöä. Yleisellä tasolla on lisäksi viitattu EU-tuomioistuimen tulkintoihin. Säätämisjärjestysperusteluissa mainittujen perustuslain säännösten ohella ehdotuksella on yhtymäkohta perustuslain 81 §:n 2 momenttiin valtion maksuista. Alajakson 12.2 otsikossa viitataan kysymykseen viranomaisen suoritteen maksullisuudesta, mutta asiaa ei käsitellä. En kuitenkaan näe tähän liittyvän valtiosääntöisiä ongelmia. Katson tarpeelliseksi tarkastella seuraavassa vielä erikseen esityksen suhdetta perustuslain 10 §:n mukaiseen luottamuksellisen viestinnän salaisuuden suojaan. Lausuttu koskee 1. lakiehdotusta ellei erikseen ole toisin mainittu.

Luottamuksellisen viestin salaisuuden suoja

Uuden kyberturvallisuuslain 23 §:ään sisältyisi ehdotus CSIRT-yksikön (Computer security incident response team) koordinoimista kyberturvallisuustietojen vapaaehtoisista jakamisjärjestelyistä sekä 28 §:ään ja 2. lakiehdotuksen 18 i §:ään ehdotukset valvovan viranomaisen tiedonsaantioikeudesta. Ehdotuksissa on kyse muun ohella oikeudesta käsitellä sähköiseen viestintään liittyvää välitystietoa ja haitallisen tietokoneohjelman tai käskyn sisältävään viestiin liittyvää tietoa. Lisäksi 21 §:ssä säädettäisiin toimivaltuudesta yleiseen viestintäverkkoon liitettyjen viestintäverkkojen ja tietojärjestelmien haavoittuvuuksien havainnoinnista.

Esityksen mukaan haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevien ehdotuksien perustuslainmukaisuuden arvioinnin kannalta ratkaisevaa on tulkinta siitä, nauttiiko haitallisen tietokoneohjelman tai käskyn sisältävä viesti luottamuksellisen viestinnän suojaa perustuslain 10 §:n 2 momentin mukaisena luottamuksellisena viestintänä siten, että perustuslain 10 § momentissa olevaa erityistä lakivarausta on sellaisenaan sovellettava, vai onko kysymys suojan ydinalueen ulkopuolelle sijoittuvasta toiminnasta, jota on arvioitava perusoikeuksien yleisten rajoitusedellytysten mukaisesti.

Esityksessä on päädytty arvioon, jossa kyberhyökkäyksen toteuttamiseksi luotu haitallisen tietokoneohjelman tai käskyn sisältävä viesti ei kuulu viestinnän luottamuksellisuuden suojan ydinalueelle, etenkään sen teknisten haittaohjelmaan liittyvien ominaisuuksien taikka automatisoidusti luodun sisällön osalta, viestinnän osapuoliksi luettavien luonnollisten henkilöiden välisen sisällön puutteen vuoksi. Esityksessä todetaan, että näin ollen kysymys ei olisi perustuslain 10 §:n 2 momentissa tarkoitetusta luottamuksellisesta viestinnästä, eli sen käsittelystä voitaisiin säätää perustuslain 10 §:n 4 momentista riippumatta. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevan sääntelyn perustuslainmukaisuutta olisi arvioitava perustuslain yleisten rajoitusedellytysten kautta siten, että sääntely on välttämätöntä, asianmukaista ja oikeasuhtaista sillä tavoiteltavien hyväksyttävien ja painavan yhteiskunnallisen tarpeen mukaisten tavoitteiden toteuttamiseksi.

Esityksen mukaan haitallisen tietokoneohjelman ja käskyn sisältävässä viestissä on usein kyse haitallisen tietokoneohjelman automaattisesti luomasta viestistä, jossa viestin lähettäjänä ei ole luonnollista henkilöä, vaan haittaohjelma tai sen ohjelmoinut taho. Viesti on pääasiallisesti semanttista sisältöä vailla oleva tekninen koneiden välinen viesti taikka haitallisen tietokoneohjelman automaattisesti luoma tai kyberhyökkäystä suorittavan tahon ennalta tuntemattomalle ja hyvin laajalle vastaanottajajoukolle lähettämä kalasteluviesti. Haitallisen

tietokoneohjelman tai käskyn sisältävän viestin lähettäjänä on taho, jonka pyrkimyksenä on toteuttaa kyberhyökkäys tai aiheuttaa haittaa viestintäverkon ja tietojärjestelmän toiminnalle tai järjestelmässä olevien henkilö- ja muiden tietojen luottamuksellisuudelle.

Lisäksi esityksessä arvioidaan, että haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittely jää viestinnän luottamuksellisuuden suojan ydinalueen ulkopuolelle. Käsittelyn arvioidaan täyttävän perusoikeuksien yleiset rajoitusedellytykset, kun huomioidaan käsittelyn tarkoitus ja tavoite suhteessa rajoituksen laatuun ja merkittävyyteen. Lisäksi NIS 2 -direktiivin täytäntöönpano edellyttää näiden tietojen käsittelemisen mahdollisuutta valvovassa viranomaisessa valvontatehtävän suorittamiseksi. Myös tältä osin esityksessä arvioidaan, että ehdotus täyttää perusoikeuksien yleiset rajoitusedellytykset. Haavoittuvuuskartoitustoiminnassa ei puolestaan esityksen mukaan kaapattaisi tai analysoitaisi osapuolten välistä viestintää.

Ehdotettu sääntely on merkityksellistä perustuslain 10 §:ssä turvatun luottamuksellisen viestinnän salaisuuden suojan kannalta. Perustuslain 10 §:n 2 momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Pykälän 4 momentin (817/2018) mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Perustuslain 10 §:ssä mahdollisuudet rajoittaa luottamuksellisen viestin salaisuutta on tarkoitettu tyhjentäväksi luetteloksi (HE 309/1993 vp, s. 54, PeVM 25/1994 vp, s. 5, ks. esim. PeVL 33/2013 vp, s. 3, PeVL 32/2013 vp, s. 3, PeVL 10/2004 vp, s. 4, PeVL 13/2003 vp, s. 4). Perustuslain 10 §:n 2 momentin säännös luottamuksellisen viestin salaisuudesta on muotoiltu väline- ja tekniikkaneutraaliksi. Kirje- ja puhelinsalaisuus on mainittu erikseen, mutta säännöksellä turvataan yleisesti kaikenlaisen luottamuksellisen viestinnän salaisuutta (HE 309/1993 vp, s. 53). Luottamuksellisen viestin salaisuutta koskevan perustuslakisääntelyn ensisijaisena tarkoituksena on suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta. Perustuslailla turvataan jokaiselle oikeus luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tietoa hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Tämä merkitsee esimerkiksi suojaa kirjeiden ja muiden suljettujen viestien avaamista ja hävittämistä sekä puhelujen kuuntelemista ja nauhoittamista vastaan. Sääntelyllä ei suojata ainoastaan viestin lähettäjää, vaan kysymyksessä on viestinnän molempien osapuolten perusoikeus (HE 309/1993 vp, s. 53–54, ks. esim. PeVL 33/2013 vp, s. 3/I, PeVL 32/2013 vp, s. 3/I, PeVL 19/2008 vp, s. 3, PeVL 59/2006 vp, s. 2, PeVL 16/2004 vp, s. 6, PeVL 10/2004 vp, s. 4–5).

Viestin sisällön lisäksi perustuslain säännöksillä suojataan myös viestin lähettäjän ja vastaanottajan tunnistamistietoja sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilymiselle. Viestin tunnistamistietojen on perustuslakivaliokunnan vakiintuneessa käytännössä katsottu jäävän luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle (ks. esim. PeVL 33/2013 vp, s. 3, PeVL 32/2013 vp, s. 3, PeVL 6/2012 vp, s. 3–4, PeVL 67/2010 vp, s. 4, PeVL 66/2010 vp, s. 7, PeVL 62/2010 vp, s. 4). Perustuslakivaliokunta on kuitenkin sittemmin katsonut EU-oikeuskäytännön valossa olevan perusteita

jossain määrin arvioida uudelleen sähköisessä viestinnässä saatavien tunnistamistietojen suojaa luottamuksellisen viestin salaisuuden näkökulmasta. Käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen (PeVL 18/2014 vp, s. 5–9). Tunnistamistietojen salaisuuden suojaan puuttuvan sääntelyn on kuitenkin täytettävä perusoikeuksien rajoittamisen yleiset edellytykset (PeVL 62/2010 vp, s. 4–5, PeVL 23/2006 vp, s. 3).

Perustuslain 10 §:n 4 momentissa on säädetty perusteet luottamuksellisen viestin salaisuuden suojan rajoittamisesta. Rajoitusperusteissa on irtauduttu rajoituksen perustumisesta rikokseen tai rikosepäilyyn. Säännöstä on sovellettu tiedustelulainsäädännön säätämisessä (PeVL 76/2018 vp, PeVL 75/2018 vp, PeVL 36/2018 vp, PeVL 35/2018 vp), mutta nämä rajoitusperusteet määrittävät luottamuksellisen viestinnän rajoitusten sallittavuutta mahdollisesti muussakin toiminnassa kuin siviili- ja sotilastiedustelussa (PeVM 4/2018 vp, s. 4). Perustuslain 10 §:n 4 momentin mukaisten rajoitusperusteiden tulkinnassa ovat keskeisellä sijalla perusoikeuksien yleiset rajoitusedellytykset. (HE 198/2017 vp, s. 34–39; PeVM 4/2018 vp, s. 6–9.)

Esityksessä on epämääräisyyttä perusoikeuksien yleisten rajoitusedellytysten soveltamisesta ja ylipäätään siitä, arvioidaanko tarkoitettua viestintää luottamuksellisena viestintänä. Esityksessä vaikutetaan omaksutun myös osin virheellinen käsitys perusoikeuden ydinalueen sekä perusoikeuksien yleisten ja erityisten rajoitusedellytysten välisestä suhteesta. Perustuslain 10 §:n 4 momentti on tuotu esille, mutta ehdotuksen suhdetta mainitun säännöksen mukaisiin rajoitusperusteisiin ei käsitellä.

Perustuslain 10 §:n 2 momentissa suojatun luottamuksellisen viestin ydinaluetta ei voida rajoittaa tavallisessa lainsäätämisjärjestyksessä, ja perusoikeuksien yleisiä rajoitusedellytyksiä sovelletaan 10 §:n 4 momentin sisältämän lakivarauksen mukaisten erityisten rajoitusedellytysten ohella. Nähdäkseni asiassa voi yhtyä esityksen arvioon siitä, että haitallisen tietokoneohjelman tai käskyn sisältävässä viestissä ei ole kysymys viestinnän osapuolten välisestä luottamuksellisen viestinnän suojan ydinalaan perinteisesti kuuluvasta viestistä, jolla olisi yksilöityä semanttista tai kommunikatiivista merkitystä osapuolille. Tästä huolimatta on kuitenkin vielä arvioitava, kuuluuko ehdotettu muutoin luottamuksellisen viestinnän suojan piiriin.

Arvioitaessa ehdotetun sääntelyn suhdetta luottamuksellisen viestinnän salaisuuden suojaan on mielestäni erityistä merkitystä syytä antaa sille, että kyse on haittaviestinnästä eikä tyypillisesti luonnollisen henkilön lähettämästä viestinnästä. Merkitystä on annettava myös sille, että sääntelyllä on tarkoitus estää toimintaa, jonka tarkoituksena on vakavasti vaarantaa juuri luottamuksellisen viestinnän suojaa sähköisessä viestinnässä. En pidä sääntelyn mahdollisesti merkitsemiä perusoikeusrajoituksia tähän tarkoitukseen nähden merkittävinä. Mielestäni tällainen viestintä voidaan sinänsä rajata luottamuksellisen viestin salaisuuden suojan ulkopuolelle vastaavaan tapaan kuin sähköisen viestinnän tunnistamis- tai välittämistietojen osalta on katsottu mahdolliseksi. Tällöin sääntelyn on täytettävä perusoikeuksien rajoittamisen yleiset edellytykset. Tältä osin perusteita on löydettävissä esityksen perustuslakijaksosta. Katson kuitenkin tarpeelliseksi nostaa esille, että ehdotettu sääntely kyberturvallisuutta koskevien riskien hallinnasta ja tähän liittyvistä tiedonsaantioikeuksista ja viestintään puuttumisesta muodostuu epäselväksi. Epämääräisyyttä jää esimerkiksi 28 §:ään tiedonsaantioikeudesta (”edellä

mainittuihin tietoihin välittömästi liittyvät tiedot"). Ylipäätään on syytä varmistua siitä, että sääntelyllä sallittava puuttuminen viestintään pystytään myös tosiasiassa kohdistamaan vain haitallisen tietokoneohjelman tai käskyn sisältämiin viesteihin ja niiden teknisten ominaisuuksien selvittämiseen.

Helsingissä 24.9.2024

Anu Mutanen, OTT, apulaisprofessori