Valtiovarainministeriö

Valtiovarainministeriön lausuntopyyntö VN/1660/2020

VALTIOVARAINMINISTERIÖN LAUSUNTOPYYNTÖ LUONNOKSESTA HALLITUKSEN ESITYKSEKSI AVOIMEN DATAN DIREKTIIVIN TÄYTÄNTÖÖNPANOA KOSKEVASTA LAINSÄÄDÄNNÖSTÄ

Yleistä

Valtiovarainministeriö on pyytänyt Suojelupoliisin lausuntoa otsikossa mainitusta luonnoksesta hallituksen esitykseksi. Esityksessä ehdotetaan säädettäväksi laki eräiden julkisten yritysten tiedon uudelleenkäytöstä sekä laki julkisin varoin tuotettujen tutkimusaineistojen uudelleenkäytöstä. Lisäksi julkisen hallinnon tiedonhallinnasta annettua lakia ja viranomaisten toiminnan julkisuudesta annettua lakia ehdotetaan muutettavaksi. Esityksellä on tarkoitus panna täytäntöön avointa dataa ja julkisen sektorin hallussa olevien tietojen uudelleenkäyttöä koskevan Euroopan parlamentin ja neuvoston direktiivin vaatimukset siltä osin kuin voimassa oleva kansallinen lainsäädäntö ei täytä niitä. Esitys liittyy osaltaan myös pääministeri Marinin hallituksen tavoitteeseen tehdä julkisen tiedon avoimuudesta koko tietopolitiikan kantava periaate sekä jatkaa määrätietoista julkisten tietovarantojen avaamista.

Sääntely kohdistuisi julkisen sektorin elinten hallussa oleviin tietoihin, julkisin varoin tuotettuihin ja tietovarannoissa julkaistuihin tutkimusaineistoihin, sekä tietyillä toimialoilla toimivien julkisten yritysten hallussa oleviin tietoihin silloin, kun julkinen yritys sallii tietojen käytön tai on velvollinen sen sallimaan.

Avoimen datan direktiivin täytäntöönpanolainsäädäntö koskisi julkisten tietojen saataville asettamista ja sen tapoja. Sääntely ei koskisi asiakirjoja, jotka ovat salassa pidettäviä, eikä sillä muutettaisi sitä lainsäädäntöä, jonka perusteella asiakirjojen salassapito määräytyy. Uusi velvoittavan luontoinen sääntely koskisi pääasiassa ns. arvokkaiden tietoaineistojen ja tiheästi päivittyvän tiedon saataville asettamista. Arvokkaat tietoaineistot, joiden tarkempi määrittely tapahtuu komission myöhemmillä täytäntöönpanosäädöksillä, tulisi asettaa saataville koneluettavassa muodossa, ja tiheästi tai reaaliaikaisesti päivittyvä tieto (dynaaminen data) tulisi pyynnöstä asettaa saataville teknisten rajapintojen avulla. Muun julkisen tiedon kuin arvokkaiden tietoaineistojen tai tiheästi päivittyvän tiedon aktiiviseen ja teknisten rajapintojen avulla tapahtuvaan saataville asettamiseen direktiivin täytäntöönpanolainsäädäntö ei velvoittaisi juurikaan nykyistä laajemmin.

Esitysluonnoksen kansallista turvallisuutta koskeva vaikutusarviointi

Esitysluonnokseen sisältyy erillinen osuus (jakso 4.2.3.4), jossa arvioidaan ehdotettujen muutosten vaikutuksia kansalliseen turvallisuuteen. Vaikutusarvioinnissa todetaan, että julkisistakin asiakirjoista voi joissakin tapauksissa olla mahdollista

niitä yhdistelemällä luoda tai saada selville tietoja, joiden sisältöä viranomainen ei alkuperäisiä asiakirjoja luovuttaessaan ole voinut tietää tai arvioida. Aikaisemmin tietoja on yhdistelty manuaalisesti fyysisistä asiakirjoista, jolloin sekä asiakirjojen saatavuus että rajalliset resurssit ovat rajoittaneet sitä, mitä tietojen yhdistelemisellä on mahdollista saada selville. Hallituksen esityksen mukaan rajapintojen laajempi käyttö lisää riskiä, että julkisista tietoaineistoista voidaan yhdistelemällä muodostaa tietoja, joiden avulla voidaan saada selville muutoin salassa pidettäviä seikkoja. Esitysluonnoksen vaikutusarvioinnissa päädytään edellä sanotusta huolimatta siihen, että hallituksen esityksellä ei ole merkittäviä vaikutuksia kansalliseen turvallisuuteen. Esitysluonnoksen mukaan syynä on se, että suurin osan yhdistelemiselle alttiista tiedoista on jo avattu koneluettavassa muodossa ja rajapintojen kautta sekä kansallisten toimien että erilaisten EU-säädösten kuten paikkatietoinfrastruktuuria koskevan INSPIRE-direktiivin ja älykkäitä liikennejärjestelmiä koskevan ITS-direktiivin myötä.

Esitysluonnoksessa julkituotu käsitys, jonka mukaan erilaisten julkisten tietojen riittävän laajan yhdistelemisen avulla voidaan paljastaa kansallisen turvallisuuden suojaamisen kannalta arkaluontoisia tietoja, on oikea. Tämä lähtökohta on omaksuttu myös vakoilurikosta koskevassa rikoslain 12 luvun rangaistussäänteleyssä. Rikoslain esitöiden mukaan vakoilurikokseen voidaan syyllistyä paitsi salassa pidettävien tietojen hankkimisella, myös siten, että erilaisista yleisesti käytettävissä olevista lähteistä saatavaa informaatiota suunnitelmallisesti yhdistellään keskenään tarkoituksena saada johtopäätöksinä tietoja, joita ei sellaisinaan ole missään yleisön saatavilla ja jotka yhdessä muodostavat vieraalta valtiolta salassa pidettävää tietoa. Olennaista vakoilurikosta koskevan rangaistussäännöksen soveltamisen kannalta ei ole pelkästään se, millaisista lähteistä tiedot hankitaan, vaan se, että tiedot sellaisina kuin ne on hankittu, muodostavat seikan, jonka tuleminen vieraan valtion tietoon voi aiheuttaa vahinkoa Suomelle rangaistussäännöksessä mainitulla tavalla (HE 94/1993 vp, s. 54).

Kiistattomana on myös pidettävä sitä, että teknisten rajapintojen laajempi käyttö ja koneluettavassa muodossa tapahtuva aineistojen julkaiseminen lisää riskiä vieraalta valtiolta salassa pidettävien tietoyhdistelmien paljastumiseen. Esitysluonnoksen kansallista turvallisuutta koskeva vaikutusarviointi vaikuttaa tätä taustaa vasten varsin suppealta, eikä johtopäätöstä, jonka mukaan esitys ei merkittävästi vaikuta kansalliseen turvallisuuteen, juurikaan perustella. Jossain määrin epäselväksi näin ollen jää, kuinka laajaan ja yksityiskohtaiseen eri tyyppisten tietoaineistojen kartoitukseen ja analyysiin johtopäätös nojaa. Erityisesti on syytä huomata, että esitysluonnoksessakin viitatussa avoimen datan direktiivin täytäntöönpanoa koskevassa Ruotsin valtioneuvoston kanslian selvityksessä (*Innovation genom information*; SOU 2020:55) kansalliselle turvallisuudelle aiheutuvia riskejä näytetään pidettävän huomattavasti moniulotteisempina.

Esitysluonnoksen erittäin tiukasta valmisteluaikataulusta johtuen on ymmärrettävää, että kansallisen turvallisuuden vaikutusarviointi on jäänyt jossain määrin pinnalliseksi. Suojelupoliisi pitää tärkeänä, että jatkovalmistelussa seikkaperäisesti ja konkreettisesti kartoitetaan, mitä eri tietoaineistoja uusimuotoinen saataville asettaminen koskisi ja mitkä saataville asettamisen seuraukset kansalliselle turvallisuudelle olisivat. Tällaisen yksityiskohtaisemman analyysin laatimiseen lienee hyvät mahdollisuudet, sillä vaikutusarviointien tuottamisesta vastaavan asiantuntijatyöryhmän toimikausi jatkuu 31.12.2021 saakka.

Arvokkaat tietoaineistot ja tiheästi päivittyvä tieto

Varsinainen velvollisuus rajapintojen avulla tapahtuvaan aineistojen saataville asettamiseen koskisi edellä todetusti vain ns. arvokkaita tietoaineistoja ja tiheästi päivittyvää tietoa. Näiden saataville asettamisesta säätäminen ei ole kansallisessa harkinnassa, vaan se perustuu direktiivin jäsenmaita velvoittavaan sääntelyyn. Saataville asettamista koskeva velvoite ei toisaalta koske arvokkaisiin tietoaineistoihin tai tiheästi päivittyvään dataan sisältyviä tietoja siltä osin kuin ne ovat kansallisen turvallisuuden suojaamiseksi tai muusta syystä säädetty salassa pidettäviksi.

Suojelupoliisi kiinnittää huomiota siihen, että teknisten rajapintojen avulla tapahtuvaa saataville asettamista koskeva velvollisuus saattaa aiheuttaa tarpeen tarkastella uudelleen eri tyyppisten tietojen salassa pidettävyyttä. Julkisuuslain 24 §:n 1 momentin 7 kohdassa säädetään rakennusten, laitosten ja rakennelmien sekä järjestelmien turvajärjestelyiden toteuttamiseen vaikuttavien asiakirjojen salassa pidettävyydestä. Momentin 8 kohdassa säädetään poikkeusoloihin varautumisesta ja 9 kohdassa valtion turvallisuuden ylläpitämisestä salassapitoperusteina. Kukin salassapitoperusteista voi tulla sovellettavaksi kriittistä infrastruktuuria koskeviin tietoihin. Olennaista tässä yhteydessä on se, että edellä mainitut salassapitosäännökset sisältävät vahinkoedellytyslausekkeen – 7 ja 9 kohdat ovat luonteeltaan salassapito-olettamaan perustuvia salassapitosäännöksiä, kun taas 8 kohta on luonteeltaan julkisuusolettamaan perustuva salassapitosäännös. Julkisuuslain 17 §:n 2 momentin mukaan asiakirjasalaisuutta koskevia säännöksiä sovellettaessa on otettava huomioon, onko salassapitovelvollisuus riippumaton asiakirjan antamisesta johtuvista tapauskohtaisista vaikutuksista vai määräytyykö julkisuus asiakirjan antamisesta johtuvien haitallisten vaikutusten perusteella vai edellyttääkö julkisuus sitä, ettei tiedon antamisesta ilmeisesti aiheudu haitallisia vaikutuksia.

Hallituksen esitysluonnoksessa mainitusti sinänsä julkisten tietojen saataville asettaminen rajapintojen avulla saattaa johtaa mahdollisuuteen yhdistellä tietoja tavalla, joka paljastaa vieraalle valtiolle Suomen kansallisen turvallisuuden kannalta olennaisia seikkoja. Rajapintojen avulla tapahtuvaa saataville asettamista harkittaessa saataville asettamisen seurauksia tulisi arvioida salassapitosäännösten sisältämien vahinkoedellytyslausekkeiden näkökulmasta. Vaikka jonkin tiedon perinteisemällä tavalla tapahtuva antaminen ei voisi johtaa vahinkoedellytyslausekkeessa tarkoitettuun seuraukseen, saattaa sen teknisen rajapinnan avulla tapahtuva saataville asettaminen tällaiseen seuraukseen johtaa. On syytä huomata, että erityisesti julkisuuslain 24 §:n 1 momentin 7 ja 9 kohtien soveltamiskynnykset ovat matalat, koska ne sisältävät salassapito-olettamaan perustuvan vahinkoedellytyslausekkeen. Tiedon antaminen edellyttää tällöin sen ilmeisyyttä, ettei salassapitosäännöksen suojaama etu vaarannu. Jos on vähäinenkin epäilys, että tähän saakka julkisiksi katsottujen tietojen teknisen rajapinnan avulla tapahtuva antaminen voi johtaa mahdollisuuteen yhdistellä niitä kansallista turvallisuutta vaarantavalla tavalla, tulisi tiedot ilmeisesti uudelleenluokitella salassa pidettäviksi. Tietojen uudelleenluokittelun kannalta merkitystä ei ole sillä, onko niissä kyse arvokkaista tietoaineistoista tai tiheästi päivittyvästä tiedosta, koska avoimen datan direktiivi ja sen sisältämä sääntely ei vaikuta niihin perusteisiin, joiden nojalla tiedon julkisuus tai salassa pidettävyys määrittyy.

Yksittäisenä säännöskohtaisena huomiona Suojelupoliisi toteaa, että julkisen hallinnon tiedonhallintalakiin ehdotettavien 24 a ja 24 b §:ien mukaan tiheästi päivittyvän tiedon ja arvokkaiden tietoaineistojen olisi pyynnöstä oltava saatavilla teknis-

ten rajapintojen avulla, jos tiedon saajalla on niihin erikseen säädetty tiedonsaantioikeus ja oikeus käsitellä niitä. Sikäli kuin ilmaisulla "tiedon saajalla on erikseen säädetty tiedonsaantioikeus" on tarkoitus viitata pääasiassa julkisuuslain 9 §:n 1 momentissa säädettyyn jokaisen oikeuteen saada tieto viranomaisen julkisesta asiakirjasta, pitää Suojelupoliisi ilmaisua jokseenkin harhaanjohtavana.

Suojelupoliisi kiinnittää myös huomiota eräiden julkisten yritysten tiedon uudelleenkäytöstä annettavaksi ehdotetun lain 3 §:n 2 momentin 4 kohdan säännökseen, jonka mukaan kyseistä lakia ei sovellettaisi sellaisiin julkisten yritysten asiakirjoihin, joiden "saatavuutta on rajoitettu muussa laissa esimerkiksi liikesalaisuuksien, valtion turvallisuuden tai henkilötietojen suojelemiseksi." Säännös perustuisi suoraan avoimen datan direktiivin 1 artiklan 2 kohdan d, f ja h kohtaan. Suojelupoliisin näkemyksen mukaan ehdotettu säännös on kriittisen infrastruktuurin suojaamiseksi tärkeä. Siltä kuitenkin käytännössä kokonaan puuttuvat soveltamista ohjaavat yksityiskohtaiset perustelut. Näin ollen avoimeksi jää esimerkiksi se, mitkä – jos mitkään – säännöksessä viitatut "muut lait" rajoittavat julkisten yritysten asiakirjojen saatavuutta valtion turvallisuuden suojelemiseksi. On selvä, että säännöksen viittauksella "muuhun lakiin" ei voida tarkoittaa julkisuuslakia ja siihen sisältyvää valtion turvallisuutta suojaavaa salassapitosääntelyä, koska julkiset yritykset ovat pääsääntöisesti julkisuuslain soveltamispiirin ulkopuolella. Mahdollista sen sijaan on, että tarkoituksena on viitata esimerkiksi sähkömarkkinalain 76 §:n 2 momentin sisältämään salassapitosääntelyyn. Säännöksen yksityiskohtaisissa perusteluissa olisi tarpeen systemaattisesti käydä läpi ne sektorikohtaiset lait, joihin säännöksen viittaus kohdistuu ja säännöksen soveltaminen siten perustuu. Tällainen systemaattinen läpikäynti myös tukisi aiemmin tässä lausunnossa esiin nostetun kansallista turvallisuutta koskevan seikkaperäisen vaikutusarvioinnin laadintaa.

Lopuksi

Muun tiedon kuin arvokkaiden tietoaineistojen ja tiheästi päivittyvän tiedon saataville asettamisen tapa olisi sen haltijana olevan viranomaisen tai julkisen yrityksen harkinnassa. Laintasoisten velvoitteiden puuttuessakin on mahdollista, että uusi sääntely tosiasiassa ohjaa viranomaisia ja julkisia yrityksiä julkaisemaan aiempaa suuremman osan tiedoistaan teknisten rajapintojen avulla. Mitä laajamittaisemmin tietoja asetetaan saataville teknisten rajapintojen avulla, sitä suurempi on riski, että niitä yhdistelemällä voidaan muodostaa salassa pidettäviä johtopäätöksiä. Erityisen vaikeasti hallittavan riskin muodostaa se, että eri viranomaiset keskenään teknisesti yhteensopivassa muodossa asettavat saataville tietoja toisistaan tietämättä ja toinen toistensa tietojen merkitystä ymmärtämättä. Ruotsin valtioneuvoston kanslian selvityksen (SOU 2020:55, s. 353) tavoin voidaan puhua ns. potentiaalisista tietoaggregaateista.

Kansalliselle turvallisuudelle vaaraa aiheuttavien riskien ja haavoittuvuuksien sekä niiden taustalla olevien monimutkaisten vaikutusketjujen arviointi ja hallitseminen on vaikeaa. Riskien minimoiminen edellyttää systemaattista ja riskilähtöistä ennalta estävää turvallisuustyötä, jossa viranomaisten ja kriittisen infrastruktuurin muiden toimijoiden toiminta on keskenään yhteen sovitettua. Tuloksellisen turvallisuustyön edellytyksenä on, että jollekin taholle on osoitettu toimivalta velvoittavasti ohjata sen toteuttamista koko yhteiskunnan tasolla.

Suojelupoliisi toteaa, että Suomessa ei tällä hetkellä ole ainakaan kovin yksiselitteisesti säädetty edellä mainitun kaltaisesta, kriittisen infrastruktuurin ja kansallisen turvallisuuden suojaamiseksi tarpeellisesta ohjausmekanismista ja siihen liit-

tyvistä viranomaisvastuista. Suomen sääntely poikkeaa varsin merkittävästi niistä lainsäädäntöratkaisuista, joihin naapurimaissa on päädytty ennalta estävän turvallisuustyön järjestämiseksi. Ruotsissa ja Norjassa kansallisen turvallisuuden suojaamiseksi tarpeellisen, koko yhteiskunnan kattavan turvallisuustyön perusteista, menettelyistä, velvollisuuksista ja vastuista on säädetty erillisissä laeissa (*Säkerhetsskyddslagen; Lov om Nasjonal Sikkerhet*). Muun muassa nyt lausuttavana oleva asia aiheuttaa Suojelupoliisin mielestä tarpeen selvittää, olisiko myös Suomessa syytä säätää tällaisen turvallisuustyön järjestämisestä erikseen.

Suojelupoliisin päällikkö
Poliisineuvos Antti Pelttari

Päälakimies Jan Sjöblom