10.10.2022

Resurssipoliittinen osasto
Kiinteistö- ja ympäristöyksikkö
Neuvotteleva virkamies Anu Sallinen ja erityisasiantuntija Jyrki Rihu

Eduskunnan puolustusvaliokunnalle

HE 140/2022 vp

Hallituksen esitys eduskunnalle laeiksi rakennetun ympäristön tietojärjestelmästä ja maankäyttö- ja rakennuslain muuttamisesta

Eduskunnan puolustusvaliokunta on pyytänyt puolustusministeriöltä kirjallista asiantuntijalausuntoa otsikossa mainitusta hallituksen esityksestä. Esityksessä ehdotetaan säädettäväksi uusi laki rakennetun ympäristön tietojärjestelmästä. Lisäksi maankäyttö- ja rakennuslakia ehdotetaan muutettavaksi.

1 Yleistä

Puolustusministeriö toteaa, että alueiden käyttöön ja rakentamiseen liittyvien tietojen saaminen valtakunnallisesti yhdestä järjestelmästä mahdollistaisi Puolustusvoimille nykyistä helpommin ajantasaisen alueiden käytön ja rakentamisen tiedon käyttämisen ja hyödyntämisen omassa toiminnassaan, joten tältä kannalta järjestelmä olisi – oikein toteutettuna ja turvallisuusnäkökulmat huomioiden – hyödyllinen myös Puolustusvoimille.

RYTJ:llä muodostuva laaja tietoaineisto sisältäisi tietoja koko yhteiskunnan elintärkeistä toiminnoista ja toimijoista sekä välttämättömistä kotimaisista infrastruktuureista ja rakenteista. Puolustushallinnon alueiden ja toimitilojen lisäksi tällaisia ovat esimerkiksi vesi- ja energia- ja elintarvikehuolto, jakeluliikenne, yleishyödylliset laitokset sekä asukkaiden terveyteen, hyvinvointiin ja toimeentuloon liittyvät toiminnot. Suojelupoliisi on määritellyt kriittiseksi infrastruktuuriksi näiden lisäksi muun muassa tietoliikenneverkot, tietovarannot, ruoka- ja lääkehuollon, liikenneverkostot, maksuliikenteen ja pankit.

Puolustusministeriön näkemyksen mukaan kaavoihin ja tietojärjestelmiin tulisi jatkossa merkitä vain sellaista tietoa, joka on koottunakin julkista tietoa. Puolustusvoimat soveltaa periaatetta, jonka mukaan käsiteltäessä julkista tai turvaluokittelematonta kokonaisuutta massana, siitä muodostuu vähintään turvallisuusluokkaa IV (TL IV, KÄYTTÖ RAJOITETTU) oleva kokonaisuus. Tällöin kokonaisuuden sisällyttäminen julkiseen tietojärjestelmään ei ole mahdollista.

Kaikkia Puolustusvoimien käytössä olevia kiinteistöjä koskeva kiinteistötieto muodostaa kokonaisuuden, josta pelkästään julkistakin tietoa analysoimalla kyetään tekemään pitkälle meneviä päätelmiä Puolustusvoimien toiminnasta. Julkisten lähteiden tiedustelun (Open source intelligence, OSINT) sekä tiedon kasautumisvaikutuksen vuoksi tämä koskee muitakin kuin salassa pidettäväksi määriteltyjä kohteita. Kaavaan esitetyistä Puolustusvoimien alueita ja toimintoja koskevista yksittäisistä aluetiedoista voi muodostua yhteen tietojärjestelmään koottuna valtakunnallisena kokonaisuutena TL IV tietoa.

Rakennetun ympäristön tietojärjestelmästä annetussa laissa (*RYTJ-laki*) on tärkeää tunnistaa kiinteistötiedon kasautumisvaikutus, suhtautua paikkatiedon suojaamiseen vakavasti ja ulottaa se koko kiinteistö- ja paikkatietoa käsittelevään toimitusketjuun. Mikäli elintärkeiden toimintojen tiedot digitoidaan ja tallennetaan tietojärjestelmään, sen tietoturvaan tulee kiinnittää erityistä huomiota. Myös tiedonsaantioikeuksien tarkkarajainen määrittäminen edellyttää ensin suojattavan kriittisen infrastruktuurin sekä siihen liittyvien suojattavien ominaisuuksien määrittelyä yhteismitallisesti ja valtakunnallisesti.

2 Uhkia ja riskejä maanpuolustuksen ja kansallisen turvallisuuden kannalta

Tietojärjestelmään kootun tiedon menettäminen esim. valtiollisen vakoilun, häiriön, onnettomuuden, kyberhyökkäyksen tai inhimillisen erehdyksen yhteydessä saattaa aiheuttaa maanpuolustukselle ja kansalliselle turvallisuudelle haittaa tai vahinkoa, joka ylittää digitalisaatiolla muutoin saavutettavat edut: kyberhyökkääjä lunastaa hyödyt haittojen realisoituessa koko yhteiskunnalle.

Tiedon vaarantuminen voi kaventaa liikkumavaraa myös maanpuolustukseen ja muuhun yhteiskunnalliseen varautumiseen liittyvän toiminnan suunnittelussa. Yleisessä tiedossa olevat haavoittuvuudet, kuten infrastruktuurin solmukohdat on huomioitava suunnittelussa. Sama koskee vaarantunutta tai jo menetettyä kiinteistötietoa. Kiinteän infrastruktuurin, kuten erityissuojattavien kohteiden tai keskeisten runkoverkostojen osalta kriittinen paikkatieto voidaan menettää vain kerran. Tästä syystä on tärkeää suojata tällaisen infrastruktuurin paikka- ja käyttötiedot.

Yhteiskunnan elintärkeiden toimintojen kehittämisestä, ylläpidosta ja varmistamisesta sekä tietojärjestelmistä ja niiden teknisistä rajapinnoista vastaavat jatkossa aiempaa laajemmin kaupalliset toimittajat eli konsulttiyritykset. Yrityksillä on lisäksi keskeinen ja yhä kasvava rooli myös rakennetun ympäristön tiedon (mm. rakennussuunnitelmien ja kaavojen) tuottajina. Uusien innovaatio- ja liiketoimintamahdollisuuksien kasvaessa kasvaa myös viranomaisten riippuvuus yksityisen sektorin toimijoista ja niiden toimitusketjuista. Tämä lisää entisestään yhteiskunnan elintärkeiden toimintojen haavoittuvuutta kyberuhkien ja –hyökkäysten kohteena. Kiinteistötiedon hallinnan kaupallistuminen asettaa yritysten turvallisuudelle, jatkuvuuden hallinnalle ja häiriötilanteisiin varautumiselle sellaisia uusia yhteiskunnallisia huoltovarmuudellisia vaatimuksia, joiden valvontaa, ylläpitoa, koulutusta ja yhteistoiminnan harjoittelua eri tilanteissa tulisi puolustusministeriön näkemyksen mukaan tarkastella tarkemmin.

Kiinteistöalan konsulttiyrityksille ominaista on fuusioituminen ja keskittyminen konserneiksi. Tällöin kertyvä yhteiskunnan keskeisten toimintojen kannalta kriittinen tietomassa lisää yritysten riskiä joutua kyberuhkien ja –hyökkäysten kohteeksi ja pahentaa seurausvaikutuksia riskien toteutuessa. Kaupallisiin toimijoihin liittyy lisäksi yrityskaupan riski. Uuden omistajan arvot ja turvallisuuskulttuuri tai liiketoimintamalli saattavat poiketa alkuperäisestä tarkoituksesta ja vaarantaa yhteiskunnan elintärkeät toiminnot. Riskien realisoituessa tietovuotojen havaitseminen, laajuuden arviointi sekä jäljittäminen on vaikeaa ja vastuukysymykset ovat vaikeita.

Paikka- ja olosuhdetiedon kehittynyt yhdistely koneoppimisen ja tekoälyn avulla on myös kannattavaa liiketoimintaa, ja ala kehittyy nopeasti. Lainsäädännön on reagoitava tähän selkeään muutokseen tiukentamalla turvallisuuden vaatimuksia. Digitaalisen tiedon väärinkäyttö ei liity vain sotilaallisen hyökkäyksen suunnitteluun, sabotaasiin, terrorismiin tai muuhun rikolliseen toimintaan. Valtiollisia uhkia ovat lisäksi mm. disinformaatio, mielipidemuokkaus, häirintä, trollaus, pelon ilmapiirin luominen ja kansalaisten luottamuksen heikentäminen.

3 Puolustusvoimien rakennusten ja rakenteiden merkitseminen rakennetun ympäristön tietojärjestelmään

Puolustusvoimien alueilla on sekä julkisia, että ei-julkisia rakennuksia ja rakenteita. Puolustusministeriön näkemyksen mukaan Puolustusvoimien rakennuksia ja rakenteita koskevia tietoja ei tule ilman välttämätöntä tarvetta viedä valtakunnallisiin tietojärjestelmiin. Vain sellainen tieto, mikä on muun yhteiskunnan kannalta välttämätöntä sisällyttää tietojärjestelmään ja Puolustusvoimien kannalta, mm. tiedon turvaluokitus huomioon ottaen mahdollista, voitaisiin sisällyttää tietojärjestelmään.

Puolustusministeriön näkemyksen mukaan Puolustusvoimien alueilla olevista rakennuksista ja rakenteista sekä muualla sijaitsevista pelkästään Puolustusvoimien toimintaa palvelevista rakenteista ei tule sisällyttää mitään tietoa rakennetun ympäristön tietojärjestelmään. Lisäksi jos jossain rakennuksessa tai rakenteessa (masto tms.) on Puolustusvoimien toimintaa tai laitteita, tietoa siitä ei tule sisällyttää

rakennetun ympäristön tietojärjestelmään, ellei tieto ole julkinen. Tietosuojasyistä myöskään Puolustusvoimien muusta julkisesta rekisterinpidosta eriytettyä kiinteistö- ja rakennustunnusjärjestelmää ei tule yhdenmukaistaa valtakunnallisten rekistereiden kanssa eikä asettaa saataville RYTJ:ään.

Puolustusministeriö katsoo, että samaa lähtökohtaa tulisi soveltaa myös niiden tilojen ja rakennusten osalta, joissa on turvallisuusviranomaisten toiminnan kannalta keskeisiä, esimerkiksi Puolustuskiinteistöt-liikelaitoksen, Puolustusvoimien kumppaneiden, kuten Suomen Erillisverkot Oy:n tai Valtion tieto- ja viestintätekniikkakeskus Valtorin TUVE, rakennuksia tai rakennelmia, kuten konesalit, viestiasemat, jne. Nämä eivät välttämättä palvele pelkästään Puolustusvoimia, mutta tietojen käsittely julkisessa tietokannassa saattaa muodostaa merkittävän riskin maanpuolustuksen lisäksi turvallisuusviranomaisten toiminnalle ja sitä kautta myös yhteiskunnan toimivuudelle.

4 Puolustusvoimien alueet kaavoissa

Puolustusvoimien alueiden ja toimintaan liittyvien vaikutusalueiden (melu- ja suoja-alueet) merkitseminen kaavoihin on hyödyllistä ja joiltain osin jopa välttämätöntä. Vaikutusalueet tulisi merkitä kaavoihin, jos Puolustusvoimien toiminnasta aiheutuu vaikutuksia Puolustusvoimien alueen ulkopuolelle, tai jos jollain Puolustusvoimien alueen ulkopuolelle tehtävällä rakentamisella voi olla vaikutusta Puolustusvoimien alueella olevaan tai sijoitettavaksi suunniteltuun toimintaan.

Edellä mainittujen alueiden merkitseminen kaavoihin turvaa paremmin Puolustusvoimien toiminta-edellytykset ja niiden kehittämismahdollisuudet, kuin se, ettei niitä merkittäisi kaavoihin. Kaavoilla vaikutetaan Puolustusvoimien alueiden ulkopuolisilla alueilla tapahtuvaan rakentamiseen. Alueita kaavoihin merkittäessä tulee kuitenkin huomioida tiedon kasaumavaikutus, jotta tiedon julkisuusluokka säilyy julkisena.

5 Tietojärjestelmään ja reksisterinpitoon kohdistuvat vaatimukset

Puolustusministeriön edellä esitetyn näkemyksen mukaan tietojärjestelmään tulisi koota ainoastaan kokonaisuutena julkista tietoa. Jos kuitenkin järjestelmään tultaisiin sisällyttämään, huomioiden tiedon kasaantumisvaikutus, Puolustusvoimiin liittyvää salassa pidettävää tai turvaluokiteltua tietoa eli muutakin kuin julkista tietoa, rakennutun ympäristön tietojärjestelmän tulee olla kokonaisuutena virallisesti auditoitu vähintään TL IV -tasolle. Tämä tulisi ottaa huomioon myös järjestelmää käyttävien henkilöiden osaamisessa, käyttöoikeuksissa ja niiden hallinnassa, sekä lokitietojen keräämisessä ja käsittelyssä. Tämä vaatimus korostuu, jos järjestelmään tultaisiin sisällyttämään, huomioiden tiedon kasaantumisvaikutus, Puolustusvoimiin liittyvää salassa pidettävää tai turvaluokiteltua tietoa eli muutakin kuin julkista tietoa. Lisäksi Puolustusvoimia koskevan turvaluokitellun tiedon käsittely ja säilyttäminen edellyttävät aina sitä käsittelevän henkilön hyväksyttyä turvallisuusviranomaisen tekemää henkilöturvaselvitystä sekä tietojen käsittely-ympäristön hallintaa.

Puolustusministeriö tuo esille, että kiinteistötietoa hallinnoidaan jo nykyisinkin usealla eri taholla ja eri järjestelmissä. Lakiehdotusta olisi sen vuoksi perusteltua edelleen kehittää arvioimalla tietojärjestelmästä ylläpidosta vastaavaa organisaatiota siten, että tarvittavat juridiset ja käytännön valmiudet sekä HE:ssä tarkoitetun julkisen hallintotehtävän hoitamiseen liittyvät vaatimukset täyttyvät, päällekkäisyyksistä luovutaan ja tietokokonaisuuden hallinta on asiantuntevaa, tarkoituksenmukaista ja tehokasta.

Lain tasolla tulisi lisäksi varmistaa, että yhteiskunnan toimivuuden kannalta elintärkeän digitaalisen tiedon turvaamisen tekniset järjestelyt, kuten fyysisen tallennuspaikan sijainti- ym. vaatimukset, hajasijoittelu ja palautumiskyky häiriötilanteissa tai valtiollisen kyvykkyyden kybersabotaasi- ja tiedustelutoiminnan varalta otetaan toiminnan järjestämisessä kokonaisuutena riittävästi huomioon.

6 Puolustusministeriön ehdotukset

Puolustusministeriö ehdottaa, että ennen rakennetun ympäristön tietojärjestelmän käyttöönottoa digitaalisen kiinteistötiedon turvallisuuden ulottuvuuksia edelleen tarkennetaan tunnistamalla ja määrittämällä yhteiskunnan elintärkeiden toimintojen kannalta kriittinen infrastruktuuri. Tässä työssä tulee huomioida myös CER-direktiivin vaatimukset sekä direktiivin täytäntöönpanon yhteydessä tehtävä kriittisen infrastruktuurin määrittelytyö. Tällaista infrastruktuuria ovat esimerkiksi johtaminen, kansainvälinen toiminta, puolustuskyky, sisäinen turvallisuus, talous, vesi- ja energiahuolto, väestön terveys, hyvinvointi ja toimintakyky ja palvelut ja talouselämä sekä henkinen kriisinkestävyys ja huoltovarmuus.

Lisäksi puolustusministeriö ehdottaa ennen lainsäädännön voimaantuloa paikkatiedon kansallisen turvallisuuden riskiarvion laatimista, joka myös huomioi yhtymäkohdat CER-direktiiviin. Riskiarvion tulisi käsittää koko toimitusketjun: valtionhallinnon, kuntasektorin sekä yritysten toimijat. Riskiarvion tulisi myös sisältää kattava tarkastelu nykyisestä paikkatiedon hallinnan kansallisesta ja EU-säädösympäristöstä, sen muutostarpeista sekä muista oikeudellisista kysymyksistä. Lisäksi sen tulisi sisältää Nato-jäsenyyden vaikutusten tarkastelu sekä paikkatiedon johtamisen ja koordinaatioon liittyvien vastuiden tarkastelu.

Kansallista turvallisuutta koskevat säännöstarkennukset sekä yhtymäpinnat CER-direktiiviin ja sen toimeenpanon kansalliseen sääntelyyn tulisi sisällyttää ao. kattolakeihin, kuten tiedonhallintalaki, aluevalvontalaki, valmiuslaki, laki paikkatietoinfrastruktuurista, julkisuuslaki tai kokonaan erillinen uusi laki. Näin muodostuisi kansallisen turvallisuuden ylätason kokonaisuus, jossa substanssisäädöksillä annettaisiin ainoastaan alakohtaiset käytännöt ja yhteensopivuusvaatimukset. Alueidenkäytön ja rakentamisen säädöskehikkoon (esim. RYTJ-lakiin) tulisi tällöin lisätä asetus, jolla määriteltäisiin tarkemmin kriittisen infrastruktuurin suojaus ja rekisterinpito kiinteistöjenhallinnan kannalta.

Puolustusministeriö ehdottaa myös, että erilaisista palveluista vapaasti saatavilla olevaa kiinteistö- ja paikkatietoa valvottaisiin. Kansallisen turvallisuuden säädösten sekä kriittistä infrastruktuuria koskevaan asetuksen nojalla tiedot voitaisiin velvoittaa poistamaan tällaisista palveluista.

7 Huomioita ehdotetuista säännöksistä

Esitetyn RYTJ-lain 1 §:n 2 momentin mukaan lakia ei sovellettaisi puolustustarkoitusta varten tapahtuvan alueidenkäytön suunnittelua ja rakentamista koskevien *salassa pidettävien tietojen* käsittelyyn. Puolustusministeriö esittää lain 1 § 2 momenttia muutettavaksi seuraavasti:

> Pykälän 2 momentissa säädettäisiin siitä, että ehdotettua lakia ei sovellettaisi puolustustarkoitusta varten tapahtuvaa alueidenkäyttöä ja rakentamista koskevien tietojen käsittelyyn *tarkemmin määritellyissä tapauksissa.*
>
> Säännös koskisi rakennusten, rakenteiden, rakennuskohteiden, laitteiden, väylien, lentopaikkojen, jakeluverkkojen ja verkostojen, kalliotilojen, maa- ja vesialueiden ja ympäristönsuojelurakenteiden alueidenkäytön ja rakentamisen tietojenkäsittelyä. Säännös koskisi myös Puolustuskiinteistöjä sekä Puolustusvoimien strategisia kumppaneita, joita ovat esimerkiksi Millog Oy ja Patria Oyj, Erillisverkot Oy ja Valtion tieto- ja viestintätekniikkakeskus Valtori.

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
kirjaamo@defmin.fi
www.defmin.fi

1 §:n 2 mom:

Lakia ei sovellettaisi puolustustarkoitusta varten tapahtuvaa alueidenkäyttöä ja rakentamista koskevien tietojen käsittelyyn kun on kyse

a) Puolustusvoimien lakisääteisten tehtävien toteuttamiseen tai tukemiseen tarkoitettuja alueita koskevien tietojen käsittelystä, jos näitä koskee Puolustusvoimien määrittämä salassapitotarve;

Perustelu:
Puolustusvoimat päättäisi Puolustusvoimien alueita koskevan tiedon salassapidon perusteista tapauskohtaisen harkinnan sekä tietojärjestelmän teknisen toteutuksen ja suojauksen perusteella.

b) Puolustusvoimien lakisääteisten tehtävien toteuttamiseen tai tukemiseen tarkoitettuja tiloja, rakennuksia ja infrastruktuuria koskevien tietojen käsittelystä, jos:
   1) tiedon tallentamisen tarve ei, mm. tiedon turvaluokitus huomioiden, ole muun yhteiskunnan kannalta välttämätön tai;
   2) kohde sijaitsee Puolustusvoimien alueella tai;
   3) kohde sijaitsee Puolustusvoimien alueen ulkopuolella ja salassapidolle on muu peruste.

Perustelu:
Salassapidon perusteena voivat olla esimerkiksi julkisuuslain 24 § 1 momentin 7-10 kohtien nojalla turvajärjestelyihin, poikkeusoloihin varautumiseen, sotilastiedusteluun, puolustusvoimien varustamiseen, kokoonpanoon, sijoitukseen tai käyttöön liittyvät tiedot.

Lisäksi puolustusministeriö kiinnittää huomiota RYTJ-lain 11 §:n 3 momenttiin, jonka muotoilu voi olla ongelmallinen. Esityksessä on tunnistettu, että henkilöön yhdistettävissä oleva kiinteistötieto, esim. osoitetiedot ovat henkilötietoa, jota on tarpeen suojata. Esityksen mukaan eduskunnan perustuslakivaliokunta kuitenkin hyväksyisi henkilötiedon haun tietoverkon kautta, mikäli sitä voitaisiin rajoittaa yksittäisiin hakuihin. Lisäksi RYTJ-lain 11 §:n 3 momentissa säädettäisiin poikkeuksesta julkisuuslain 16 §:n 3 momenttiin. Sen perusteella SYKE:lla olisi oikeus luovuttaa henkilötietoja ilman, että luovutuksensaajalla on oikeus käsitellä tietoja. Esitetyn 11 §:n 3 momentin mahdollistama tiedonsaanti metatiedon tasollakin olisi erinomainen tietolähde tiedusteluorganisaatioille. Vaikka tiedonhakuja on tietoturvasyistä esitetty rajattavaksi yksittäishakuihin, on erittäin oleellista arvioida, mihin tarkoituksiin tietoja luovutettaisiin ja onko rekisterinpitäjällä tosiasiallisia teknisiä keinoja rajoittaa esim. ohjelmistobottien avulla tehtävien tietohakujen määrää. HE:ssä todetaan tietojen yhdistelystä, ettei SYKE:lla rekisterinpitäjänä ole mahdollisuutta valvoa luovuttamiensa tietojen jatkokäyttöä enää sen jälkeen, kun tiedot on luovutettu. Tällöin on todennäköistä, ettei muillakaan viranomaisilla ole riittävää kykyä tai toimivaltaa suorittaa tällaista valvontaa.

Postiosoite
Postadress
Postal Address
Puolustusministeriö
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
kirjaamo@defmin.fi
www.defmin.fi