

Asia: VN/27452/2020-OM-548

Julkisuuslain salassapitoperusteiden uudistustarpeiden kartoitus

Lausunnonantajan lausunto

Mitkä ovat mielestänne nykyisten julkisuuslain 24 §:n salassapitoperusteiden kehittämistarpeet? Puuttuuko nykyisistä salassapitosäännöksistä jotain olennaista? Kuvailkaa ja perustelkaa kehittämistarvetta mahdollisimman konkreettisesti.

Yleisesti

Laki viranomaisten toiminnan julkisuudesta on kunnan toiminnassa keskeinen laki. Vaikka julkisuuslaki on vuodelta 1999, julkisuuslain 24 §:n salassapitosäätely ja soveltamiskäytännöt on koettu melko toimiviksi.

Julkisuusperiaate on avoimen hallinnon tärkeä lähtökohta. Samalla riskit julkisuusperiaatteen väärinkäytölle ovat digitalisaation myötä kasvaneet merkittävästi. Julkisuuslain salassapitosäätely ei huomioi riittävästi nykyistä toimintaympäristöä, teknologian mahdollisuuksia eikä globaalia turvallisuustilannetta.

Julkisuuslain salassapitoperusteissa on ollut soveltamisen kannalta hyvä, että keskeinen salassapitoa koskeva säätely on koottu julkisuuslakiin. On toivottavaa, että julkisuuslakiin on jatkossakin koottu salassapitoperusteet, vaikka myös muussa lainsäädännössä on salassapitoa koskevia säännöksiä. Kun julkisuuslakia sovelletaan kunnan toiminnassa laajasti, selkeyden tarve korostuu. Kaikki julkisuuslakia kunnissa soveltavat henkilöt eivät ole juristeja, vaan julkisuuslakia soveltavat työssään myös esimerkiksi kasvatuksen ja opetuksen hallinnon, maankäytön ja rakentamisen, elinvoiman, omistajaohjauksen, taloushallinnon, henkilöstöhallinnon, asiakirjahallinnon, turvallisuuden ja varautumisen, sisäisen tarkastuksen ja julkisten hankintojen asiantuntijat. Tampereen kaupunki on koonnut tähän lausuntoon asiantuntijoiden konkreettisia esimerkkejä julkisuuslain salassapitoperusteiden soveltamisesta. Salassapitoperusteiden tulisi olla selkeitä ja yksiselitteisiä koskien myös tiedon julkiseksi tuloa.

Julkisuuslain voimaantulon jälkeen lain soveltamisympäristö on muuttunut. Digitalisaatio, asianhallinnan järjestelmät, sähköpostin ja muiden järjestelmien käyttö ja tekoälyn kehitys ovat muuttaneet toimintaympäristöä. Esimerkiksi GDPR, tiedonhallintalaki ja EU:n digi- ja datasäätely ovat aiheuttaneet kysymyksiä julkisuuslain soveltamisesta. Julkisuuslain salassapitoperusteet tulee

arvioida ottaen huomioon toimintaympäristön muutokset ja julkisuuslain voimaantulon jälkeinen lainsäädäntö.

Julkisuuslain salassapitosäännösten kokonaistarkastelussa on tärkeää arvioida nykyistä enemmän yksityisyyden ja henkilötietojen suojaa. Tietojen käsittelyyn ja luovuttamiseen liittyy teknologian mahdollisuuksien takia merkittäviä riskejä. Kunnissa joudutaan arvioimaan tietojen luovuttamista useissa käytännön tilanteissa, joihin liittyy tulkinnanvaraisuutta, esimerkiksi lapsia ja nuoria, päiväkodin tai koulun oppilaita koskevat tiedot.

Viranomaisten välinen keskustelu ja tietojenvaihto tehdään usein sähköpostilla tai muita järjestelmiä käyttäen. Järjestelmiä on paljon ja niihin jää erilaisia jälkiä käydyistä keskusteluista ja tietojenvaihdoista. Tulkinnat esimerkiksi sähköpostien julkisuudesta ja salassapidosta ovat perustuneet lainsäädännön lisäksi oikeuskäytäntöön ja laillisuusvalvojien ratkaisuihin, ja näiden osalta perusteet tulisi kirjata julkisuuslakiin.

Julkisuuslain salassapitoperusteiden soveltamisessa on koettu, että monet käsitteet vaatisivat tarkempaa määrittelyä, esimerkiksi kriittinen infrastruktuuri, tiedot henkilön terveydentilasta ja mitä tietoja voi käsittää liikesalaisuus.

Turvallisuus ja varautuminen

Salassapitoperusteissa tulee ottaa huomioon turvallisuuteen ja varautumiseen liittyvät salausperusteet nykyistä paremmin ja mahdollistaa turvallisuuteen liittyvien tietojen, paikkatietojen, rakennusten turvallisuustietojen ym. salaaminen. Turvallisuutta koskevista salassapitoperusteista tulee ottaa huomioon, että myös tietojen yhdisteleminen voi muodostaa turvallisuusriskin.

Kriittinen infrastruktuuri tulee käsitteenä määritellä. Myös yleisten alueiden ja yleisökäytössä olevien rakennusten turvallisuuteen liittyvät salausperusteet on tarpeen määritellä. Vallitsevassa turvallisuustilanteessa esimerkiksi rakennetun ympäristön osalta julkisuuslain salassapitosäännöksiä tulisi voida soveltaa nykyistä laajemmin.

Kuntien teknisellä sektorilla syntyy paljon kriittistä dataa ja sen vuoksi tarvittaisiin nykyistä selkeämmät määritelmät, jotta salassa pidettävät tiedot osataan tunnistaa ja ne on mahdollista salata. Kriittistä infrastruktuuria koskevaa tietoa on asiakirjojen ohella enenevässä määrin tietokantamuotoisena ja koneluettavassa formaatissa. Rakennusten yksityiskohtien julkisuus voi vaarantaa kriittisten kohteiden turvallisuusjärjestelyjä. Julkisuuslain salassapitoperusteiden tulee mahdollistaa kriittisten kohteiden tietojen salassapito. Toisaalta kuntien maankäytön ja rakentamisen prosesseissa syntyy suunnitelmia ja muita asiakirjoja, joita ei ole perusteltua määritellä salaiseksi, mutta joita ei ole esimerkiksi kriittisen infrastruktuurin turvaamisen näkökulmasta tarkoituksenmukaista luovuttaa kaikille.

Nykyinen turvallisuusluokittelu ”julkinen” ja ”salainen” ei vastaa kaikilta osin käytännön tarpeita. Tarvittaisiin määrittelyjä tilanteisiin, joissa tieto on voi olla julkinen, mutta tietoa ei kuitenkaan julkaistaisi yleisessä tietoverkossa. Tällaisia olisivat muun muassa monet paikkatiedot ja infrastruktuuria koskevat tiedot. Yhtenä ratkaisuna voisi olla uusi julkisen ja salaisen välillä oleva salassapitoluokka, jolloin tiedon antaminen olisi viranomaisen harkinnassa. Tiedon antaminen edellyttäisi tiedonsaajan tunnistamista ja tiedonsaannin perustetta. Tarkoituksena olisi estää

turvallisuuteen ja varautumiseen liittyvien tietojen, esimerkiksi kriittisten paikkatietojen päätyminen väärin käsiin. Viranomaisella tulisi olla mahdollisuus rajata tiedonsaantioikeutta esimerkiksi maantieteellisesti tai käyttää muutoin harkintaa tietojen antamisessa.

Voimassa olevan julkisuuslain 24.1 §:n 7 kohta koskee turvallisuusjärjestelyjä. Olisi perusteltua harkita, tulisiko kohdan koskea turvallisuuteen liittyviä tietoja, eikä ainoastaan turvallisuusjärjestelyjä. Valmiussuunnitelmat tulisi voida määritellä salassa pidettäväksi. Nykyisin kunnat ovat joutuneet julkaisemaan ainakin osan valmiussuunnitelmistaan.

Salassapitosäännöksiin tulisi lisätä kohta, jossa mahdollistetaan nykyistä paremmin yksityiskohtaisen paikkatiedon salaaminen, esimerkiksi kriittiseen infrastruktuuriin liittyviä kohteita kuten valvomorakennukset, muut rakennelmat, tietoliikenne- ja sähkökaapit jne., joiden sijaintitieto ei yksinään välttämättä täytä nykyistä salassapidon kriteeriä, mutta jonka havaitaan olevan hybridivaikuttamiseen liittyvän urkinnan tai rikollisen toiminnan tiedustelun kohteena. Vastaavasti tulisi arvioida tietoaineistoja, tekoälypohjaisia järjestelmiä, IoT-laitteiden sisältämiä tietoja ja niiden salassapitoa.

Salassa pidettävään turvallisuustietoon valtionhallinnossa liittyy tiedonhallintalain 18 §:n mukainen vaatimus asiakirjojen turvallisuusluokittelusta ja niihin turvallisuusluokkaa koskevasta merkinnästä sen osoittamiseksi, minkälaisia tietoturvaluustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Kun tarkastellaan salassapitosäännöksiä, tulisi arvioida, millaisia vaikutuksia turvallisuusluokittelun laajentamisella olisi kuntien ja hyvinvointialueiden salassa pidettävään tietoon. Turvallisuutta koskevien salassa pidettävien asiakirjojen käsittelyn yhtenäistäminen parantaisi turvallisuuteen liittyvän tiedonvaihdon edellytyksiä.

Kriittistä infrastruktuuria koskevia asiakirjoja on kertynyt kunnille huomattavia määriä. Aineiston asiakirjakohtainen salaaminen on työmäärältään erittäin suuri ja olisi toivottavaa, että tietoja voitaisiin salata laajempina kokonaisuuksina.

Sisäinen tarkastus

Käytännössä ongelmalliseksi koettuja soveltamisen kannalta ovat salassapitoperusteet, joiden soveltamisessa tehdään tulkintaa tiedon antamisen seurauksista, kuten 15 kohdassa ”asiakirjat, jotka sisältävät tietoja viranomaisen tehtäväksi säädetystä tarkastuksesta tai muusta valvontatoimeen liittyvästä seikasta, jos tiedon antaminen niistä vaarantaisi valvonnan tai sen tarkoituksen toteutumisen tai ilman painavaa syytä olisi omiaan aiheuttamaan vahinkoa asiaan osalliselle”.

Sisäisen tarkastuksen suunnitelmien, raporttien ja muiden tietojen julkisuus ja julkiseksi tulo tulisi arvioida lainsäädännössä nykyistä selkeämmin ottaen huomioon, että tarkastuksen onnistuneessa toteuttamisessa myös luottamuksellisuuteen liittyvä tiedonsaanti on tärkeää. Ilmoittajansuojelulain ja julkisuuslain soveltamiseen liittyvät tulkinnat tulisi arvioida salassapitosääntelyn uudistamisen yhteydessä.

Henkilöstöhallinto

Julkisuuslain 24 §:n 1 momentin 29 kohdan mukaan palkitsemisessa eurot ovat julkisia henkilökohtaisen lisän osalta sekä arviointijärjestelmä on julkinen, mutta perusteita henkilökohtaiselle lisälle ei voi avata, koska se sisältää arviointia. Yleiset perusteet käsitellään työpaikalla yleisellä tasolla. Tässä kuitenkin läpinäkyvyys olisi hyväksi, jotta kriteerit voitaisiin avata henkilökohtaiselle lisälle myös henkilön kohdalla eikä vain yleisiä kriteereitä. Lisäksi samoin voidaan todeta kertapalkkion osalta.

Henkilökohtaisiin syihin perustuvassa irtisanomispäätöksessä usein arvioidaan henkilökohtaisia ominaisuuksia. Salassapitosäännösten soveltamisalan ulottaminen irtisanomistilanteisiin selkeyttäisi tilannetta.

Varoitusten ja huomautusten julkisuus ei ole kunnassa yksiselitteistä ja lainsäädäntöä tulisi tältä osin selkeyttää.

Rekrytoinnissa hakemusasiakirjat ovat julkisia, kun ne ovat saapuneet viranomaiselle. Julkisuus voi nostaa hakemisen kynnystä, koska hakijoiden nimet tulevat julki.

Henkilötunnus

Tulisi arvioida henkilötunnuksen lisäämistä julkisuuslain 24 §:n salassa pidettäviin tietoihin. Henkilötunnus ei ole julkisuuslain 24 §:ssä tarkoitettu salassa pidettävä tieto eikä erityisiin henkilötietoryhmiin kuuluva tieto.

Tietosuojalain 29 §:ssä säädetään henkilötunnuksen käsittelystä. Tietosuojalaki määrittelee tilanteet, joissa henkilötunnusta saa käsitellä. Henkilötunnusta ei tule merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

Henkilötunnuksen käyttäminen tietojärjestelmissä voi lisääntyä sähköisen tiedoksiannon ensisijaisuuden myötä (suomi.fi-liityntäpinta edellyttää henkilötunnusta henkilön tunnistamiseen).

Tietopyynnöt

Journalistiset ja myös muut, laajatkin tietopyynnöt ovat kunnan toiminnassa melko yleisiä. Joissakin tapauksissa kunnalle osoitetut tietopyynnöt voivat sisältää satoja asiakirjoja (tietopyynnön kohteena voi olla esimerkiksi kaikkien asuinrakennusten energiatodistusten asiakirjat). Laajoihin tietopyyntöihin liittyy usein riskejä yksityiselämän ja henkilötietojen suojaan liittyen, esimerkiksi päiväkodit, koulut, oppilaitokset. Lainsäädännön tulisi mahdollistaa laajaan tietopyyntöön vastaamiseen liittyviä rajoituksia.

Digitalisaatio on myös aiheuttanut kysymyksiä siitä, miten paljon tietoa kunnan tulee koota järjestelmistä tietopyyntöön vastaamiseksi.

Olisi perusteltua harkita muutosta, ettei tietopyyntöä kaikissa tilanteissa voisi esittää anonyyminä ja että tietopyyntö tulisi määritellyissä tilanteissa perustella. Koska julkishallintoon kohdistuu riskejä tietojen kalastelulle ja hybridivaikuttamiselle, on tärkeää, että mahdollisuuksia reagoida myös näihin

uhkiin ja toisaalta mahdollisuuksia suojella julkishallintoa parannetaan, vaikka kysymyksessä ei olisikaan salassa pidettävä tieto.

Jos julkisuuslain soveltamisalaa muutettaisiin mietinnössä ehdotetulla tavalla (Oikeusministeriön julkaisuja 2023:32, lakiehdotuksen 5 §), millaisia muutoksia tämä edellyttäisi salassapitoperusteisiin? Kuvaile ja perustelkaa muutostarvetta mahdollisimman konkreettisesti.

Julkisuuslain soveltamisalan laajentamisessa tulee ottaa huomioon yhteiskunnan kriittisistä toiminnoista vastaavien julkisomisteisten konserniyhtiöiden, kuten vesihuolto, jätehuolto, energia- ja sähköhuolto, ruokahuolto ja ict salassapitoon liittyvät kehittämistarpeet. Kaupungin turvallisuuteen liittyvät keskeisesti kriittisen infrastruktuurin ja muiden kriittisten toimintojen yhtiöiden turvallisuusasiat.

Kriittinen infrastruktuuri (kuten vesihuolto, jätehuolto, energiahuolto ja ruokahuolto) toimii pääosin julkisomisteisten konserniyhtiöiden toimintana. Näihin toimintoihin on havaittu kohdistuvan viime aikoina hybridihaavoittamista, kuten esimerkiksi jatkuvaa tiedustelua niin tietoverkkojen kautta kuin fyysisestikin. Julkisuuslain soveltamisalan laajentaminen koskemaan yhteiskunnan kriittisistä toiminnoista vastaavia julkisomisteisiä yhteisöjä voi muodostaa turvallisuusriskin.

Liikesalaisuuksien määrittely on koettu edelleen vaikeaksi.

Oletteko tunnistaneet tietojen tai asiakirjojen salassapitoa koskevaa erityislainsäädäntöä, joka on ristiriidassa julkisuuslain salassapitosäännösten kanssa? Jos julkisuuslain soveltamisalaa muutettaisiin mietinnössä ehdotetulla tavalla (Oikeusministeriön julkaisuja 2023:32, lakiehdotuksen 5 §), aiheutuisiko soveltamisalan muutoksesta konkreettisia ristiriitoja nykyisen erityislainsäädännön kanssa tai tarvetta tarkentaa erityislainsäädäntöä?

Tulee arvioida EU:n digi- ja datasäädösten, esimerkiksi paikkatietojen ja julkisuuslain välinen suhde. Lisäksi tulee ottaa huomioon kriittistä infrastruktuuria koskevien tietojen käytön ja salaamisen tulkinnat, Inspire, HVD.

Uusi alueidenkäyttölaki edellyttää, että asema-, yleis- ja maakuntakaavat tuotetaan kansallisen tietomallin mukaisessa, koneluettavassa muodossa. Näiden tietojen julkisuus on tarpeen määritellä selkeästi. Kaavaprosessiin liittyvien kriittistä infrastruktuuria koskevien tietojen julkisuus ja salassapito tulisi määritellä.

Julkisuuslain ja GDPR:n rajapinnan on koettu käytännön soveltamisessa aiheuttavan tulkintakysymyksiä ja epävarmuutta käytännön työssä.

Työsuojeluprosessien yhteydessä syntyvien asiakirjojen julkisuuteen tulisi kiinnittää huomiota. Työsuojeluasiakirjojen, kuten työsuojeluilmoitusten, salassapidosta säädetään laissa työsuojelun valvonnasta ja työpaikan työsuojeluyhteistoiminnasta (44/2006). Kyseisen lain 10 §:n mukaan tietyt ilmoituksiin liittyvät tiedot ovat salassa pidettäviä valvontaviranomaisen hallussa. Tätä salassapitosäännöstä ei kuitenkaan sovelleta valvontaviranomaisten ulkopuolella, minkä vuoksi vastaavat tiedot ovat kunnallisissa viranomaisissa pääsääntöisesti julkisia. Oikeuskäytännössä on kuitenkin katsottu, että myös muut kuin valvontaviranomaiset voivat rajoittaa asianosaisjulkisuutta ilmoittajan suojaamiseksi. On kuitenkin huomattava, että erityislainsäädäntöön sisältyvä kategorinen salassapitosäännös muodostaa olennaisen aste-eron verrattuna tilanteisiin, joissa salassapito perustuu harkintaan. Nykyinen sääntelyn epäyhtenäisyys on johtanut tulkintavaikeuksiin ja vaihtelevaan ohjeistukseen työsuojeluprosessien käsittelystä kunnissa ja muissa kuin valvontaviranomaisissa. Sääntelyä olisi tarpeen yhdenmukaistaa. Erityisesti tulisi ottaa huomioon

työsuojeluprosessien luonne ja niihin liittyvä tiedon arkaluonteisuus. Yhdenmukainen ja selkeä sääntely edistäisi oikeusturvaa, viranomaistoiminnan ennakoitavuutta sekä henkilöstön luottamusta työsuojelujärjestelmään.

Julkisuuslain soveltamisalan ehdotettuun laajentamiseen liittyen tulee arvioida, mikä on julkisuuslain soveltamisalan laajentamisen ja osakeyhtiölain sääntelyn välinen suhde. Osakeyhtiölain mukaan yhtiön johdon on huolellisesti toimien edistettävä yhtiön etua. Osakeyhtiön hallituksella ja toimitusjohtajalla on velvollisuus olla julkistamatta sellaisia tietoja, joiden antaminen voi olla yhtiölle vahingollista.

Aittala Pauliina

Tampereen kaupunki - Konsernijohtaja Juha Yli-Rajala 5.6.2025 § 115