PERUSTUSLAKIVALIOKUNNALLE

Asia: HE 225/2020 vp Hallituksen esitys eduskunnalle laiksi tartuntatautilain väliaikaisesta muuttamisesta annetun lain muuttamisesta

Esitän lausuntonani kunnioittaen seuraavaa.

Esityksen tarkoituksena on mahdollistaa tartuntaketjujen katkaisua tehostavan mobiilisovelluksen eli Koronavilkun rajat ylittävä toimivuus muiden vastaavien sovellusten kanssa. Tartuntatautilakiin lisättäisiin uudet säännökset tietojärjestelmän rajat ylittävän käytön yhteydessä tapahtuvasta henkilötietojen luovuttamisesta toisen EU:n jäsenvaltion, Euroopan talousalueeseen kuuluvan valtion tai Sveitsin nimetylle kansalliselle viranomaiselle tai viralliselle elimelle. Esityksessä ehdotetaan lisäksi lain voimassaolosäännöstä muutettavaksi siten, että laki olisi voimassa 31.12.2021 saakka.

Asia on valtiosääntöoikeudellisesti merkittävä erityisesti yksityiselämän suojan kannalta, johon sisältyy myös henkilötietojen suoja. Perustuslain 10 §:n lähtökohtana on yksilön oikeus elää elämäänsä ilman aiheetonta puuttumista.

Ehdotuksen kuvaamalla tietojärjestelmällä on vaikutuksia henkilötietojen suojaan. Ollakseen hyväksyttäviä, niiden tulee täyttää tietyt edellytykset, joista osa johtuu kotimaisesta valtiosääntöoikeudesta, osa taas kansainvälisestä normistosta. Keskeinen merkitys on unionin yleisellä tietosuoja-asetuksella.

Koronavilkun käyttö on vapaaehtoista. Tämä ei perustusvaliokunnan mukaan kuitenkaan poista tarvetta varmistaa, että sääntely kokonaisuudessaan luo riittävät edellytykset arkaluontoisten henkilötietojen suojan tosiasialliselle toteutumiselle (PeVL 20/2020 vp, s. 6). Myös nyt ehdotettavan rajat ylittävän tietojen vaihdon on esityksen mukaan tarkoitus olla vapaaehtoista, mutta esitystä on silti tarkasteltava kokonaisuudessaan, jotta voidaan arvioida yksityisyyden suojan ja henkilötietojen suojan toteutumista.

Käsittelyn oikeusperuste

Tietosuoja-asetuksen mukaan henkilötietojen käsittelylle on oltava oikeusperuste, eli laillinen syy. Hallituksen esityksen mukaan ehdotetun tietojärjestelmän yhteydessä tapahtuvan henkilötietojen käsittelyn oikeusperuste on asetuksen 6 artiklan 1 kohdan e

alakohta, jonka mukaan käsittely on sallittua, kun se on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.

Kun käsittely perustuu yleiseen etuun tai julkisen vallan käyttämiseen, tulee käsittelyn perusteesta säätää joko unionin oikeudessa tai rekisterinpitäjään sovellettavassa jäsenvaltion lainsäädännössä. Nykyinen tartuntatautilain 4 a luku ei kaikilta osin kata henkilötietojen käsittelyä rajat ylittävissä tilanteissa. Tästä on nyt säädettävä lailla.

Silloin kun käsittely oikeutetaan edellä kuvatun yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdalla, tulee jäsenvaltion lainsäädännön täyttää yleisen edun mukainen tavoite ja oltava oikeasuhtainen sillä tavoiteltuun oikeutettuun päämäärään nähden, kuten 6 artiklan 3 kohdassa säädetään. Ehdotetun rajat ylittävän käsittelyn voidaan vallitsevassa epidemiatilanteessa katsoa täyttävän yleisen edun mukaisen tavoitteen. Eurooppalaisella yhteistyöllä pyritään hillitsemään pandemiaa, sekä osittain mahdollistamaan vapaa liikkuvuus. Ehdotusta voidaan myös pitää oikeasuhtaisena päämääräänsä nähden, ottaen huomioon esityksen kuvaamat hyödyt.

Tietojärjestelmän yhteydessä käsiteltäisiin terveyttä koskevia tietoja. Niitä pidetään yleisen tietosuoja-asetuksen 9 artiklassa tarkoitettuina erityisiin henkilötietoryhmiin kuuluvina tietoina, kotimaisessa käsitteistössämme arkaluonteisina tietoina. Tällaisten tietojen käsittely on lähtökohtaisesti kiellettyä. Käsittely on 9 artiklan mukaisesti sallittua vain silloin, kun sille on jokin 9 artiklan 2 kohdassa tarkoitettu erityinen käsittelyperuste.

Hallituksen esityksen mukaan terveystietoja käsiteltäisiin 9 artiklan 2 kohdan i alakohdan perusteella. Sen mukaan käsittely on sallittua, jos se on tarpeen kansanterveyteen liittyvän yleisen edun vuoksi, kuten vakavilta rajat ylittäviltä terveysuhkilta suojautumiseksi. Tietojärjestelmän yhteydessä tapahtuva terveystietojen käsittely voidaan nähdäkseni perustaa tähän tietosuoja-asetuksen kohtaan. Edellytyksenä on kuitenkin asiaa koskeva lainsäädäntö, jossa tulee säätää asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn oikeuksien ja vapauksien, erityisesti salassapitovelvollisuuden suojaamiseksi. Siten nyt esitettyä lainsäädäntöä on tarkasteltava sen mukaisesti, täyttääkö se nämä edellytykset.

Lakiehdotuksessa tarkoitetuissa rajat ylittävissä tilanteissa tietojärjestelmän käytön yhteydessä olisi välttämätöntä käsitellä tietoa tietojärjestelmän rajat ylittävään käyttöön liittyvistä maista ja pseudonyymisten tunnisteiden alkuperämaista. Lisäksi olisi välttämätöntä voida luovuttaa tartunnastaan ilmoittaneiden henkilöiden pseudonyymiset tunnisteet toisen osallistuvan maan viranomaiselle. Kyseessä olisi

nykysääntelyyn nähden uudenlaisesta käsittelystä, joka koskisi osittain myös terveyteen liittyviä tietoja (tieto tartunnasta).

Ottaen huomioon tietojärjestelmällä tavoiteltu laajaan henkilöjoukkoon liittyvä henkilötietojen käsittely ja terveystietojen käsittely, on tietojärjestelmää koskevassa sääntelyssä syytä säätää henkilötietojen käsittelystä yksityiskohtaisesti ja tarkkarajaisesti. Lisäksi on säädettävä asianmukaisista suojatoimista yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan i alakohdan mukaisesti. Silti on syytä muistaa, että tietosuoja-asetuksesta itsestään seuraa lukuisia vaatimuksia rekisterinpitäjälle ja henkilötietojen käsittelijälle henkilötietojen käsittelyyn liittyen. Kaikesta kansallisen lainsäätäjän ei siis tarvitse säätää, eikä sääntelyliikkumavara sitä mahdollistakaan.

Käsittelyn minimointi

Käsittelyn minimointi on keskeinen tietosuoja-asetukseen sisältyvä periaate. Ehdotetun lakimuutoksen mukaan käsiteltävien henkilötietojen joukko rajattaisiin vain käyttötarkoituksen kannalta välttämättömiin tietoihin ja ne yksilöitäisiin lainsäädännössä. Henkilötietojen enimmäissäilytysaika olisi melko lyhyt, sillä henkilötiedot olisi poistettava tai tuhottava viimeistään 21 vuorokautta siitä, kun ne olisi tallennettu, tai viimeistään kun tietojärjestelmä poistetaan käytöstä. Käsiteltävät tiedot olisivat pääosin pseudonyymisiä, mikä vähentää henkilötietojen suojaan kohdistuvia riskejä, sillä yksittäisen käyttäjän yksilöiminen olisi niiden pohjalta hyvin vaikeaa.

Komission täytäntöönpanoasetuksen 7 a artiklan mukaan yhdyskäytäväpalvelun kautta vaihdettavat ja siinä käsiteltävät pseudonymisoidut henkilötiedot voivat sisältää ainoastaan tiettyjä tietoja, kuten kansallisten mobiililaitteissa käytettävien kontaktien jäljitys- ja varoitussovellusten välittämät avaimet enintään 14 päivän ajalta ennen avaimien lataamista ja avaimiin liittyvät lokitiedot avainten alkuperämaassa käytettyjen teknisten eritelmien protokollan mukaisesti. Siinä käsiteltäisiin toki myös tietoa infektion todentamisesta. Vaikutta siltä, että yhdyskäytäväpalvelun kautta jaettavat henkilötiedot on rajattu vain välttämättömään.

Pseudonymisointi

Koronavilkku käsittelee pseudonymisoituja tietoja. Järjestelmään kerätään kyllä myös muita kuin pseudonymisoituja tietoja tartuntatautilain 43 c §:n mukaan. Näitä ovat nimi, puhelinnumero, kotikunta ja tarvittaessa tilapäinen asuinpaikka ja oiretiedot. Näitä ei kuitenkaan käsitellä käyttäjien puhelimissa olevissa sovelluksissa.

Rajat ylittävät henkilötiedot, joita käsitellään komission yhdyskäytäväpalvelussa, olisi pseudonymisoitu, mikä vähentää sekä tietosuojaan että tietoturvaan liittyviä riskejä. Ehdotuksen perusteella vaikuttaa siltä, että puhelimissa olevat mobiilisovellukset keräisivät myös rajat ylittävissä tilanteissa pelkästään pseudonymisoituja tietoja. Sovelluksen käyttäjä ei myöskään saisi tietää minkä maan sovelluksen kanssa ilmoituksen aiheuttama kohtaaminen on tapahtunut. Mobiilisovelluksella tallennettaisiin vain muiden lähistöllä olevien käyttäjien pseudonymisoituja tunnisteita.

On tärkeää, että tunnisteesta ei ilmene käyttäjän henkilöllisyys, eikä tunnistetta voi yhdistää henkilöön ilman kohtuuttomia toimenpiteitä. Koska pseudonyymi tunniste voi kuitenkin potentiaalisesti olla yhdistettävissä henkilöön, on sekin henkilötieto. Asian valtiosääntöoikeudellisen arvioinnin kannalta olennaista kuitenkin on, että pseudonyymisiin tunnisteisiin pohjautuvaan järjestelmään liittyy huomattavasti pienempiä riskejä kuin sellaiseen järjestelmään, jossa henkilö olisi tunnistettavissa suoraan. On myös tärkeää, etteivät käyttäjät saa hallituksen esitykseen sisältyvän kuvauksen perusteella tietoa toisista käyttäjistä, eikä heille päädy muiden käyttäjien henkilötietoja. Sääntelyn perusratkaisut ovat tältä osin tietosuoja-asetuksen mukaisia.

Vapaaehtoisuus

Henkilötietojen suojalle aiheutuvia riskejä vähennetään jossain määrin käytön vapaaehtoisuuden ja käyttäjän tiedollista itsemääräämisoikeutta edistävien toimenpiteiden avulla. Ketään ei pakoteta ottamaan Koronavilkkua käyttöön, vaan sen käyttö perustuu vapaaehtoisuuteen. Esityksen mukaan suostumus toimisi lisäsuojatoimena myös rajat ylittävissä tilanteissa. Henkilöltä kysyttäisiin suostumus ennen tietojen luovuttamista toisen maan sovelluksesta vastaavalle viranomaiselle tai muulle viralliselle elimelle. Suostumusta ei olisi pakko antaa tätä tarkoitusta varten. On tärkeää, että henkilö voisi silti jatkaa Koronavilkun käyttämistä kotimaassa. Lisäksi kukin voi koska tahansa poistaa sovelluksen käytöstä.

Tietosuoja-asetuksen johdanto-osan 32 kohdan mukaan henkilötietojen käsittelyn oikeuttava pätevä suostumus on vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla henkilö hyväksyy henkilötietojensa käsittelyn. Tällaisia suostumusta ilmentäviä toimia ovat esimerkiksi se, että henkilö rastittaa ruudun vieraillessaan internetsivustolla, valitsee teknisiä asetuksia tai esittää minkä tahansa muun lausuman tai toimii tavalla, joka selkeästi osoittaa, että hän hyväksyy henkilötietojensa käsittelyn.

Vapaaehtoisuus ei kuitenkaan riitä ehdotetun käsittelyn oikeusperusteeksi. Perustuslakivaliokunta on suhtautunut pidättyväisesti siihen, että suostumusta käytetään perusoikeuksiin puuttumisen oikeutusperusteena. Perusoikeussuojaa ei voida millaisessa asiassa tahansa jättää riippumaan asianomaisen suostumuksesta. Perustuslakivaliokunta on myös edellyttänyt lakiin säännöksiä suostumuksen antamisen ja sen peruuttamisen tavasta, sekä siitä miten suostumuksen aitous varmistetaan (PeVL 27/1998 vp, s. 2; PeVL 19/2000 vp, s. 3).

Perustuslakivaliokunnan mukaan epätasapainoisessa tilanteessa kuten terveydenhuollon asiakaspalvelussa annettava suostumus ei välttämättä ole aidosti vapaaehtoinen, eikä tällaisessa tilanteessa asiakkaalla ole aina tosiasiallisia mahdollisuuksia harkita suostumuksen merkitystä. Valiokunta on myös kiinnittänyt tämänkaltaisissa sääntely-yhteyksissä huomiota siihen, että suostumuksen on perustuttava riittävään tietoon (PeVL 1/2018 vp, s. 10).

Siten voidaan katsoa, ettei hallituksen esityksessä kuvattu henkilötietojen käsittely voi tapahtua suostumuksen perusteella, vaan se on oikeutettava jollain muulla tavalla. Kuten yllä on todettu, yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohta ja terveystietojen osalta 9 artiklan 2 kohdan i alakohta soveltuvat käsittelyn oikeuttaviksi perusteiksi. Vapaaehtoisuus ei silti ole järjestelmän valtiosääntöoikeudellisen tarkastelun kannalta yhdentekevää. Se täydentäisi käsittelyn hyväksyttävyyttä ja toimisi, kuten hallitus esittää, suojatoimena.

Koronavilkkua koskevassa lausunnossaan perustuslakivaliokunta totesi, että mikäli käsittely ei perustu tietosuoja-asetuksen 7 artiklan mukaiseen suostumukseen, on säädettävä täsmällisesti suostumuksen antamisen ja peruuttamisen tavasta sekä suostumuksen aitouden ja tietoon perustuvuuden varmistamisesta. Suostumuksesta on myös ilmettävä, ettei sitä ole annettu sosiaali- ja terveydenhuollon asiakaspalvelutilanteessa tai muussakaan viranomaismenettelyssä (PeVL 20/2020, s. 8).

Ehdotettua rajat ylittävää henkilötietojen käsittelyä varten laaditussa 43 i §:ssä säädettäisiin, että

> henkilötietojen luovuttaminen 2 momentin mukaisesti edellyttää käyttäjän suostumusta. Suostumus annetaan sovelluksessa. Suostumuksesta tulee käydä ilmi, että se on annettu vapaaehtoisesti ja nimenomaisesti sekä tietoisena siitä, mihin tarkoituksiin tietoja voidaan luovuttaa ja käyttää. Suostumuksesta on myös käytävä ilmi, ettei sitä ole annettu sosiaali- ja terveydenhuollon asiakaspalvelutilanteessa eikä viranomaismenettelyssä.

Muotoilu vastaa perustuslakivaliokunnan vaatimuksia varsin hyvin.

Johtopäätökset

Vaikuttaa siltä, että esityksessä kuvattuun rajat ylittävään järjestelmään sisältyvä henkilötietojen käsittely on suunniteltu yleisen tietosuoja-asetuksen periaatteita noudattaen. Esityksen perusoikeusrajoituksilla voidaan katsoa olevan hyväksyttävä tavoite. Ottaen huomioon tietojen käsittelyn lähtökohtana oleva pseudonyymisten tietojen käsittely, henkilötietojen käsittelyn minimointi, tietojen lyhyt säilytysaika sekä tietojen luovutuksen perustuminen henkilön omaan tahdonilmaisuun, voidaan ehdotettuja perusoikeusrajoituksia pitää oikeasuhtaisuusvaatimuksen mukaisina. Kaiken kaikkiaan ehdotetussa laissa säädettäisiin henkilötietojen käsittelystä varsin yksityiskohtaisesti ja tarkkarajaisesti. Näillä perusteilla katson, että ehdotus voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä.

Helsingissä 26.11.2020
Susanna Lindroos-Hovinheimo