Viite:
Oikeusministeriön lausuntopyyntö 17.6.2024, VN/26111/2023

Asia:
Tietosuojalainsäädännön kokonaisuudistuksen koordinaatioryhmän väliraportti

Yleistä

Oikeusministeriön selvitys on tehty tietosuojalainsäädännön kokonaisuudistuksen toteuttamiseksi. Kokonaisuudistuksen tavoitteena on parantaa julkisten palveluiden järjestämistä siten, että lainsäädännöstä tunnistetaan sellaiset henkilötietojen käsittelyä koskevat säännökset, jotka vaikuttavat viranomaisten tiedon liikkuvuuteen ja julkisten palveluiden järjestämiseen. Hankkeen puitteissa on tarkoitus toteuttaa tarvittavat lainmuutokset, joissa otetaan huomioon perustuslaista johtuvat vaatimukset ja Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (tietosuoja-asetus) sallima sääntelyliikkumavara.

Nähdäkseni väliraportti on varsin kattava ja informatiivinen. Siinä on tunnistettu useita tietosuojasääntelyn hankaluuksia ja tulkinnanvaraisia kohtia. Kiinnitän silti huomioita eräisiin seikkoihin, joita tulisi pohtia lisää.

Yleisenä huomiona raportissa pistää silmään se, että Euroopan unionin tuomioistuimen (EUT) oikeuskäytäntöä on tarkasteltu hyvin vähän. Ajatuskulkuna lienee se, että unionin tuomioistuimen näkemykset vaikuttavat tietosuoja-asetuksen ja muun EU-sääntelyn, mutta eivät koske kansallisen lainsäädännön tulkintaa. Näin luonnollisesti onkin, mutta välillisesti EUT:n ratkaisuilla on huomattava vaikutus siihen, miten tietosuojasääntelyä kansallisesti

PL 20, 00023 Valtioneuvosto Puhelin 0295 16001 kirjaamo.okv@gov.fi

www.oikeuskansleri.fi

tulkitaan, sovelletaan ja säädetään. On jossain määrin erikoista, ettei raportissa esille nostettuja asioita tarkastella – taikka arvioida – EUT:n ratkaisukäytännön valossa. Kenties se vaihe uudistustyössä on vasta edessä, mutta voidaan perustellusti olla sitä mieltä, että etusijaperiaatteesta ja tietosuojasääntelyn voimakkaista EU-oikeudellisista liitoksista johtuen EUT:n käytäntö olisi hyvä olla mukana lainvalmistelussa alusta alkaen. Tämä ei tarkoita sitä, että tuomioistuimen kaikki ratkaisut otettaisiin sellaisinaan lainsäädäntötyön pohjaksi. Edellyttäisin pikemminkin huolellista analyysiä siitä, milloin, miten ja missä määrin EUT:n ratkaisut on otettava huomioon kansallista sääntelyä uudistettaessa.

Sähköinen asiointi viranomaisissa

Sähköinen asiointi viranomaisissa on yksi raportin tärkeimmistä teemoista tehtävänannosta johtuen. Tältä osin on huomattava, että lainsäädännöllinen kehikko on varsin hankala. Sovellettaviksi tulevat ainakin tietosuoja-asetus, tietosuojalaki, julkisuuslaki, tiedonhallintalaki, sähköinen asiointilaki, laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista sekä laki digitaalisten palvelujen tarjoamisesta. Ei ole yllättävää, että tämän lainsäädännön keskinäissuhteiden ja yhteisvaikutusten hahmottaminen on useissa viranomaisissa vaikeaa. Aiheesta ei ole erityisen paljon myöskään tulkintaa helpottavaa tutkimusta.

Lainsäädännön sekavuus ja pirstaleisuus lienee yksi tärkeimmistä syistä sille, ettei sähköistä asiointia ja julkishallinnon digitalisointia aina voida edistää kovin helposti. Vaikuttaa siltä, että raportissa kyllä tunnistetaan tilanne, mutta siinä ei esitetä toimia sen helpottamiseksi. Johtopäätöksissä ehdotetaan ylipäänsä varsin vähän lainsäädäntötoimia. Nähdäkseni jatkovalmistelussa olisi hyvä kiinnittää enemmän huomiota siihen, millä tavoin lainsäädäntöä voitaisiin selkeyttää.

Esimerkkinä ajankohtaisesta pulmasta, joka saattaisi vaatia tarkempaa reflektointia on viranomaisten käyttämät digitaaliset viestintätavat tilanteissa, joissa viestintään sisältyy erityisiä henkilötietoryhmiä tai salassa pidettäviä tietoja. Käytännöt vaihtelevat julkishallinnon eri puolilla. Voimassa oleva lainsäädäntö aiheuttaa tulkintahankaluuksia, jotka todennäköisesti näkyvät käytännössä. Esimerkiksi tiedonhallintalain 14 §:n 1 momentin mukaan salassa pidettävien tietojen siirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin hän pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. Jos salassa pidettävien tietojen vastaanottaja on luonnollinen henkilö, hänet on tunnistettava jollakin luotettavalla menetelmällä, esimerkiksi vahvaa sähköistä tunnistusmenetelmää käyttämällä. Toisaalta, tunnistautuminen lisää henkilötietojen keräämistä ja käsittelyä, mikä voi olla vastoin tietosuojasääntelyn minimointiperiaatetta. Voimassa olevan lainsäädännön mukaan viranomainen voikin vaatia digitaalisessa palvelussa käyttäjältä sähköistä tunnistamista vain, jos se on tarpeen palvelun tai sen tietosisältöön liittyvien käyttöoikeuksien varmistamiseksi tai palvelussa tehtävään toimeen liittyvien oikeusvaikutusten

vuoksi (laki digitaalisten palvelujen tarjoamisesta 6 §). Lisäksi tunnistautuminen ei aina ole kaikille henkilöille mahdollista, mistä seuraa yhdenvertaisuus- ja saavutettavuusongelmia.

Nähdäkseni oikeustila on jossain määrin epäselvä siltä osin, missä kaikissa tapauksissa tunnistautumista taikka vahvaa tunnistautumista edellytetään viranomaisten asioidessa henkilöiden kanssa. Näkemykseni on myös, että aiheesta on varsin erilaisia tulkintoja ja käytäntöjä eri viranomaisissa. Lainsäädännön selkeyttämistä tulisi harkita.

Tietosuojalain soveltamisala

Tietosuojalainsäädännön kehittämisen yhteydessä saattaa olla tarpeen miettiä myös sitä, onko tietosuojalain soveltamisalan määrittely toteutettu tarkoituksenmukaisesti. Lain 2 §:stä seurannee tietyillä aloilla hankalia tulkintatilanteita muun muassa siitä, milloin on sovellettava tietosuojalakia ja milloin rikosasioiden tietosuojalakia, ja milloin on sovellettava tietosuoja-asetusta.

Esimerkkinä voidaan mainita Rajavartiolaitos. Henkilötietojen käsittelyyn Rajavartiolaitoksessa sovelletaan käsittelytarkoituksesta riippuen joko yleistä tietosuoja-asetusta ja sitä täydentävää tietosuojalakia tai rikosasioiden tietosuojalakia (ja epäsuorasti rikosasioiden tietosuojadirektiiviä). Tämä johtuu siitä, että tietosuojalain 2 §:n 1 momentin mukaan tietosuoja-asetusta ja tietosuojalakia sovelletaan myös sellaiseen käsittelyyn, joka jää asetuksen 2 artiklan soveltamisalan ulkopuolelle. Siten kansallinen ratkaisu on ollut se, että tietosuoja-asetuksen soveltamisala on laajempi kuin EU-oikeudessa määritelty tietosuoja-asetuksen soveltamisala. Lopputulos on jossain määrin merkillinen, sillä tietosuoja-asetuksen soveltamisala ulottuu laajemmalle kuin itse asetus määrittelee. Tällä laajemmalla alueella herää hankalissa tulkintatilanteissa kysymyksiä esimerkiksi siitä, soveltuvatko myös EUT:n ratkaisut oikeuslähteinä, vai mistä tulkinta-apua on saatavissa.

Rajavartiolaitoksen toimintaan sovelletaan ePrivacy-direktiiviä ja lakia sähköisen viestinnän palveluista. Lisäksi merkittävä on luonnollisesti Rajavartiolaitoksen henkilötietolaki (639/2019). Merkityksellisiä ovat myös ainakin Rajavartiolaitoksen rikostorjuntalaki (108/2018), aluevalvontalaki (755/2000), merenkulun turvatoimilaki (485/2004) ja pakkokeinolaki (806/2011). Lisäksi, jotta henkilötietojen suojaa Rajavartiolaitoksella voidaan arvioida kokonaisuutena, tulee ottaa huomioon lainsäädäntö, joka koskee tietojen luovutuksia. Yleislakina toimii silloin julkisuuslaki, mutta useista yllä mainituista laeista ilmenee, että Rajavartiolaitoksella on sääntelyn nojalla oikeus luovuttaa tietoja salassapitosäännösten estämättä monille viranomaisille. Kaiken kaikkiaan henkilötietojen suoja on varsin monimutkainen kokonaisuus, josta Rajavartiolaitosta koskeva normisto on vain yksi konkreettinen esimerkki.

Huomionarvoista eri instrumenttien soveltamisalojen kannalta on myös EUT:n ratkaisukäytäntö siltä osin, kuin se laajentaa tietosuoja-asetuksen soveltamisalaa EU-oikeuden soveltamisalan ulkopuolelle. Vaikka asetuksen 2 artiklan 2 kohdan a alakohdassa on säädetty, ettei asetusta sovelleta henkilötietojen käsittelyyn, jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan, on EUT suhtautunut melko sallivasti asetuksen soveltamiseen esimerkiksi kansallisten parlamenttien toiminnassa (ks. C-272/19 Land Hessen sekä varsinkin C-33/22 Österreichische Datenschutzbehörde). Sama tendenssi on nähtävillä tapauksissa, joissa EUT on ottanut kantaa kansallisen turvallisuuden määrittelyyn, vaikka kansallinen turvallisuus on lähtökohtaisesti unionin lainsäädäntövallan ulkopuolella (ks. esim. C-511/18, C-512/18 ja C520/18 La Quadrature du Net ym.; C-793/19 ja C-794/19 SpaceNet ja Telekom Deutschland; C-205/21 Ministerstvo na vatreshnite raboti; C-162/22 A.G. v Lietuvos Respublikos generalinė prokuratūra).

Koska EUT tulkitsee tietosuojainstrumenttien soveltamisalaa varsin laajasti, herää lisää kysymyksiä siitä, miten stabiili tietosuojalain 2 §:n 1 momentin tulkinta voi olla. Momentin mukaan tietosuoja-asetusta sovelletaan myös alueilla, jotka eivät kuulu unionin oikeuden soveltamisalaan, mutta tuo unionin oikeuden soveltamisala laajenee siinä määrin, että myös momentin merkitys saattaa olla muutoksessa. Kaiken kaikkiaan näkisin, ettei tietosuojalain 2 § ole muotoilultaan selkein mahdollinen.

Tietojen liikkuvuus viranomaisilta toisille

Raportissa on käsitelty tietojen liikkumista viranomaisilta toisille ja monet käytännön soveltamisongelmat tuodaan hyvin esille. Silti lisää hankaluutta aiheuttanee käyttötarkoitussidonnaisuuden periaate ja sen erinäiset tulkinnat EU-oikeudessa ja kansallisessa oikeudessa. Näkemykseni on, että käyttötarkoitussidonnaisuuden periaatteeseen viitataan lainsäädännössä ja esitöissä, mukaan lukien valiokuntien lausuntokäytännössä, melko epäjohdonmukaisesti. Ajoittain se nousee merkittävään asemaan argumentaatiossa, ajoittain ei. Periaatteen tulkintaan liittyviä ongelmia on raportissa tunnistettu sivuilla 53-55 ja 57, mutta nähdäkseni voisi olla tarpeen pohtia myös, onko niille tehtävissä jotain.

Oikeudellisesti erityinen asiaryhmä ovat tilanteet, joissa lainsäädäntö sallii (tai edellyttää) tietojen liikkumisen viranomaisten välillä kansallisen turvallisuuden perusteella. Näissä tilanteissa oikeustila on sikäli epäselvä, että on ajoittain hankalaa arvioida, miten ja missä määrin EU-oikeudellinen normisto soveltuu (ks. yllä tietosuojalain ja tietosuoja-asetuksen soveltamisalasta).

Kotimaisesta sääntelystämme löytyy myös ratkaisuja, joissa tietojen siirtoa kansallisen turvallisuuden perusteella ei ole määritelty tai rajattu kovin selkeästi. Esimerkkinä voidaan mainita rahanpesun selvittelykeskuksesta annetun lain 4 §:n 4 momentti. Sääntelystä ei saa

selvää, mitkä ovat ne viranomaiset, joille tietoa voidaan kansallisen turvallisuuden perusteella luovuttaa. Lainsäädännön johdonmukaisuuden kannalta ongelmallista lienee myös se, ettei tietojen luovuttamista ole sidottu välttämättömään. Esimerkki kuvastanee sitä, että kansallisen turvallisuuden perusteella on lainsäädännössä tehty erinäisiä poikkeuksia, jotka eivät aina ole yhdenmukaisia taikka täytä perusoikeusrajoitusten täsmällisyyden ja tarkkarajaisuuden vaatimuksia.

Tietojen luovutusten osalta merkityksellinen sääntelykohde saattaa olla myös tietojen luovutusten tapa, johon ei eri alojen sektorikohtaisessa lainsäädännössä aina kiinnitetä huomiota. Kuten perustuslakivaliokunta on katsonut, esimerkiksi katseluyhteys ei sovellu sellaiseen luovutukseen, jossa viranomaisen on arvioitava luovutettavan tiedon tapauskohtaista välttämättömyyttä (ks. esim. PeVL 11/2024 vp). Voisi olla tarpeen kiinnittää huomiota myös siihen, missä tilanteissa tekninen rajapinta tai katseluyhteys voi toimia tiedon luovutuksen tapana ja missä ei. Selvityksessä voisi tarkemmin pohtia sitä, edellyttääkö tämä teema lainsäädäntötoimia joko yleislakien tai erityislakien tasolla.

Henkilötietojen siirrot kolmansiin maihin on oma kokonaisuutensa, jossa oikeustila on epäselvä ja käytäntö vaihtelevaa. Tämäkin on todettu raportissa, jossa esimerkiksi pilvipalveluihin liittyvät ongelmat nostetaan esiin useaan otteeseen. Raportissa ei kuitenkaan esitetä näkemystä siihen, miten ongelmiin voitaisiin lainsäädännössä vastata. Epäselvää lienee myös se, missä tilanteissa ja miten paljon kansallista liikkumavaraa aiheen tiimoilta löytyy, ottaen huomioon tietosuoja-asetuksen V luku.

Julkisuusperiaate ja oikeudenkäynnin julkisuus

Raportissa todetaan paikoitellen, että tietosuojan ja julkisuusperiaatteen yhteensovittaminen on eri hallinnonaloilla koettu vaikeaksi. Näkemykseni mukaan näin tosiaan on. Tätä on luontevinta tarkastella käynnissä olevan julkisuuslain uudistamisen yhteydessä. Näkisin silti, että tietosuojan ja julkisuusperiaatteen välinen jännite on merkittävä asia myös tietosuojalainsäädännön uudistamista pohdittaessa.

Raportista saa sen kuvan, ettei julkisuusperiaate ole tietosuojasääntelyn uudistamishankkeen kannalta erityisen merkittävä. Nähdäkseni olisi kuitenkin hyödyllistä, että tässäkin yhteydessä kartoitettaisiin kansallisen liikkumavaran käyttö huolellisesti, erityisesti niissä raameissa, joita EUT:n oikeuskäytäntö asettaa.

Yleisellä tasolla oikeustila on tietosuojan ja julkisuusperiaatteen yhteensovittamisen kannalta tällä hetkellä Suomessa varsin erikoinen. Tietosuojalainsäädännössä, kuten tietosuojalain 28 §:ssä, viitataan julkisuuslakiin ja muuhun julkisuussääntelyyn. Julkisuuslaissa, erityisesti 16 §:ssä, sen sijaan viitataan tietosuojasääntelyyn. Tämä viittausten kierre aiheuttaa

laintulkitsijoille, niin virkamiehille kuin tuomareillekin, ymmärrettävän ongelman, sillä soveltamistilanteissa kumpikin periaate on oikeuslähteiden valossa yhtä vahvasti säännelty, mutta sisällöllisesti toisensa määrittämä.

Tulkintatilannetta ei luonnollisesti helpota se, että molemmat periaatteet on suojeltu myös perustuslain tasolla. EU-oikeudessa sen sijaan vain tietosuoja on tarkalleen ottaen konstitutionaalisella tasolla suojeltu sen saadessa tukea sekä SEUT 116 artiklasta että perusoikeuskirjan 8 artiklassa. EU-oikeuden näkökulmasta on siten luontevaa, että tietosuoja saa voimakkaamman suojan, mikä näkyy myös EUT:n ratkaisuissa. Kotimaisessa oikeudessamme näin ei kuitenkaan ole, vaan julkisuusperiaate on yhtä voimakkaasti suojeltu kaikessa viranomaistoiminnassa. Tämä pitkään hankaluuksia aiheuttanut tulkintapulma olisi nähdäkseni syytä ottaa keskiöön, mikäli tietosuojasääntelyä uudistetaan. En näe, että tilanne ratkeaa pelkästään julkisuuslakia uudistamisella.

Oikeudenkäynnin julkisuus on mainittu erikseen raportin sivulla 35. Oikeudenkäynnin julkisuus saa suojaa sekä perustuslain 21 §:ssä että EU-oikeuden tasolla perusoikeuskirjan 47 artiklassa. Siten oikeuslähteiden tasolla kumpikin periaate on lähtökohtaisesti vahvasti suojeltu sekä kansallisessa oikeudessa että EU-oikeudessa. Tästä huolimatta EUT:n tuoreessa käytännössä on ollut tapana antaa painoarvoa tietosuojalle punnintatilanteissa (esim. C-268/21 Norra Stockholm Bygg ja erityisesti C-740/22 Edemol Shine Finland). Myös kotimaisessa oikeudessamme on ajoittain ollut havaittavissa tilanteita, joissa tietosuojaa on painotettu oikeudenkäynnin julkisuuden sijaan kenties yksipuolisesti. Nähdäkseni asia vaatii selvittämistä. On mahdollista, että kotimaisia lainsäädäntötoimia tarvitaan, jotta perustuslain 21 §:n asettamat vaatimukset toteutuvat. Näkisin, että tähän oikeudenkäynnin julkisuuden toteutumista koskevaan selvitystyöhön olisi syytä ryhtyä mahdollisimman pian. En näe perusteluja sille, että asiassa odotetaan julkisuuslakiin ehdotettavien muutosten valmistumista.

Tietosuoja-asetuksen 23 artikla

Havaintojeni mukaan tietosuoja-asetuksen 23 artikla, joka antaa jäsenvaltioille muissa artikloissa nimenomaisesti mainitun liikkumavaran lisäksi yleistä liikkumavaraa, on Suomessa alikäytetty. Artikla on raportissa mainittu muun muassa sivuilla 30 ja 48. Sen soveltuvuutta olisi kuitenkin tarkoituksenmukaista arvioida yksityiskohtaisemmin monissa eri yhteyksissä. Sääntelyliikkumavaran löytäminen on erityisen tärkeää niissä tilanteissa, joissa liikkumavaran käyttämisellä kyetään turvaamaan perustuslaissa säädettyjä oikeuksia. Näissä tilanteissa tulee kansallisella lainsäätäjällä olla valmius ja asiantuntemus tulkita EU-oikeutta, mukaan lukien tietosuoja-asetusta siten, että perusoikeuksia pystytään suojelemaan. Nähdäkseni EUT:n käytäntö antaa tähän kyllä eväitä, sillä tuomioistuin on toistuvasti toistanut (joskaan ei aina aivan johdonmukaisesti soveltanut) ohjenuoraa, jonka mukaan tietosuoja ei ole absoluuttinen oikeus, vaan edellyttää punnintaa muiden oikeuksien kanssa.

Sektorikohtaista lainsäädäntöä ja sen uudistamistarvetta pohdittaessa on nähdäkseni tarpeen myös arvioida sääntelytekniikkaa 23 artiklaan liittyen. Avoimia kysymyksiä ovat muun muassa se, miten erilaisissa erityislaeissa tai niiden esitöissä olisi syytä viitata 23 artiklaan. Voi olla, ettei eri hallinnonalojen lainvalmistelijoilla ole tietoa taikka juuri kokemustakaan 23 artiklan yksityiskohdista, mistä syystä siihen harvemmin viitataan. Voisi olla tarpeen kartoittaa, tarvitaanko tältä osin yhtenäisten käytäntöjen kehittämistä eri hallinnonalojen lainvalmistelijoiden keskuudessa.

Erityislainsäädännön tarve

Raportissa todetaan perustuslakivaliokunnan aikanaan toteamaa näkemys, jonka mukaan erityislainsäädäntöä tietosuojasta tulisi välttää. Se tulee varata niihin tilanteisiin, joissa henkilötietojen suojaa on tarpeen vahvistaa käsittelyyn liittyvien riskien vuoksi (ks. esim. PeVL 14/2018 vp, s. 4–5). Tosiasia kuitenkin on, että tietosuoja-asetus itsessään sekä digitalisoitunut yhteiskunta yleisesti edellyttävät runsasta erityislainsäädäntöä, jolloin pääsääntönä ei voida pitää sitä, että erityislainsäädäntöä tulisi välttää. Jotta sektorikohtaista erityislainsäädäntöä voitaisiin karsia tai säätää vähemmän kuin nykyisin, tulisi tietosuojalakia uudistaa niin, että se olisi huomattavasti kattavampi ja yksityiskohtaisempi. On epäselvää, mikä tämän sääntelyratkaisun etu olisi. Lisäksi on otettava huomioon, ettei perustuslakivaliokunta itsekään enää vaikuta suhtautuvan kriittisesti erityislainsäädäntöön. Siitäkin syystä voi olla aika hyväksyä, että erityislainsäädäntöä tarvitaan ja tullaan tarvitsemaan jatkossakin.

Tietosuojalain 4 §:n 1 momentin 2 kohta

Raportin johtopäätöksissä korostuu jonkin verran pohdinta siitä, tulisiko tietosuojalain 4 §:n 1 momentin 2 kohtaa muuttaa. Selvityksessä on käynyt ilmi, että useilla hallinnonaloilla tietosuojalain 4 §:n 1 momentin 2 kohta on koettu vaikeaksi tulkita. Raportin johtopäätöksissä todetaan kuitenkin mielestäni viisaasti, että lainkohdan muuttaminen vaatii tarkkuutta ja harkintaa, jotta tulkintaepäselvyydet eivät lisäänny entisestään.

Tietosuoja-asetukseen liittyvät EU-oikeudelliset uudistukset

EU:n tasolla on vireillä lainsäädäntöaloite, joka uudistaisi tietosuoja-asetukseen liittyviä prosessuaalisia järjestelyjä (COM(2023) 348 final). Tämä tuleva asetus voisi olla syytä ottaa huomioon lainsäädännön kehitystyön yhteydessä. Asetuksella tulee olemaan vaikutusta ainakin tietosuojavaltuutetun toimintaan. Olisi hyvä arvioida myös sitä, missä määrin asetus saattaa aiheuttaa muutoksia tietosuojaoikeuksien tehokkaaseen suojaan. Kiinnittäisin huomiota varsinkin niihin hankaluuksiin, joita eri maiden eri kielillä asioivat henkilöt saattavat kohdata asioidessaan toisten jäsenmaiden tietosuojaviranomaisten kanssa.

Tämä asiakirja on allekirjoitettu sähköisesti.

Oikeuskansleri Tuomas Pöysti

Esittelijäneuvos Susanna Lindroos-Hovinheimo