

Jakelun mukaan

VN/10855/2024

Poliisihallituksen lausunto luonnoksesta hallituksen esitykseksi sähköisestä tunnistamisesta, luottamuspalveluista ja eurooppalaisesta digitaalisesta identiteetistä annettua EU:n asetusta täydentäväksi lainsäädännöksi

Valtiovarainministeriö pyytää Poliisihallituksen lausuntoa luonnoksesta hallituksen esitykseksi eduskunnalle sähköisestä tunnistamisesta, luottamuspalveluista ja eurooppalaisesta digitaalisesta identiteetistä annettua EU:n asetusta täydentäväksi lainsäädännöksi.

Euroopan parlamentti ja neuvosto antoivat 11.4.2024 asetuksen (EU) 2024/1183 asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehityksen vahvistamisen osalta (jäljempänä eIDAS-muutosasetus). eIDAS-muutosasetus on sellaisenaan jäsenvaltioissa sovellettavaa oikeutta. Asetus jättää kuitenkin eräissä asioissa jäsenvaltioille kansallista liikkumavaraa. Lisäksi uudistetussa eIDAS-muutosasetuksessa on joitain velvoitteita jäsenvaltioille, kuten eurooppalaisen digitaalisen identiteetin lompakon tarjoaminen, kansallisen valvontaelimen ja kansallisen yhteyspisteen nimeäminen, jotka edellyttävät kansallista täydentävää lainsäädäntöä. Hallituksen esityksellä ehdotetaan säädettäväksi edellä mainituista asioista, jotta uudistettua eIDAS-muutosasetusta voidaan Suomessa soveltaa tehokkaasti.

Esityksessä ehdotetaan lisäksi lompakon kanssa ensimmäisen yhteensopivan sähköisen todistuksen toteuttamista Suomessa, ja se olisi poliisin tuottama digitaalinen henkilöllisyystodistus. Lisäksi esityksessä tehdään kansallisista tarpeista johtuvia sähköisen asioinnin ja vahvan sähköisen tunnistamisen käytön turvallisuutta lisääviä sekä lainsäädännön ajantasaistamiseksi tarpeellisia muutoksia.

Poliisihallitus on ollut mukana hallituksen esityksen valmistelussa ja kannattaa esitettyjä muutoksia. Tässä lausunnossa on esitetty sellaisia seikkoja, joihin hallituksen esityksen jatkovalmistelussa tulisi kiinnittää huomiota.

Vahvan sähköisen tunnistamisen avulla kansalaiset voivat turvallisesti vahvistaa henkilöllisyytensä erilaisissa sähköisissä palveluissa ja lisäksi sähköisten asiointipalveluiden tarjoajat voivat tunnistaa asiakkaansa. Suomessa nykyisin yleisesti käytettävä vahva sähköisen tunnistamisen väline on pankkien tarjoamat pankkitunnukset. Tunnusten kalastelu ja väärinkäytökset ovat lisääntyneet vuosi vuodelta merkittävästi.

Uudet pankkiasioitiin liittymättömät tunnistusvälineet ovat omiaan lisäämään sähköisen asioinnin turvallisuutta ja estämään petosrikollisuuden kasvua. Rikostorjunnallisesta näkökulmasta on toivottavaa, että pankkiasiointiin pohjautuva sähköinen tunnistautuminen korvautuu muilla luotettavilla tunnistautumisen menetelmillä.

Poliisin tietoon tuli vuonna 2024 noin 4000 tietojen kalasteluun liittyvää rikosta, joiden rikosvahinko oli arviolta noin 37.8 miljoonaa. Tämän lisäksi pankit ja poliisi tekevät tiivistä yhteistyötä rikosten estämiseksi. Pankit osaltaan tekevät aktiivisesti töitä asiakkaisiinsa kohdistuvien petosten estämiseksi. Finanssiala ry:n pankeilta keräämien tietojen mukaan suomalaisilta yritettiin huijata 107,2 miljoonan euron edestä rahaa vuonna 2024. Vuonna 2023 määrä oli 76,9 miljoonaa euroa. Esitetyt luvut edustavat todennäköisesti vain murto-osaa todellisista aiheutuneista vahingoista.

Samalla laajenee tunnistuspalveluiden tarjoaminen perinteisten pankkien ja viranomaisten ulkopuolelle erilaisille palveluntarjoajille. Rikosten ennalta estämisen, paljastamisen ja selvittämisen kannalta olennaista on tunnistuspalveluiden palveluntarjoajien ja palveluiden riittävä luotettavuus ja turvallisuus, viranomaisten ja palveluntarjoajien välinen yhteistyö rikosten estämiseksi sekä se, miten hallinnan menettämiseen ja väärinkäyttötilanteisiin voidaan puuttua rikosten ja niistä aiheutuvien vahinkojen estämiseksi ja selvittämiseksi sekä palveluita tarjottaessa, että niitä käytettäessä. Tunnistusvälineitä koskevassa sääntelyssä on turvattava viranomaisille mutta myös rikosten uhreille riittävät keinot puuttua väärinkäyttötilanteisiin.

Asian merkitys ja tilastotiedot huomioiden lakiehdotus käsittelee varsin pintapuolisesti tunnistusvälineiden hallinnan menettämistä, riskejä ja siitä aiheutuvia vahinkoja sekä viranomaisten toimivaltuuksia väärinkäyttötilanteissa. Kuitenkin on oletettavaa, että kuten ennenkin, myös nämä uudet tunnistamisen välineet ovat rikollisten mielenkiinnon kohteena, kalasteltavissa ja väärinkäytettävissä.

Tunnistuspalveluiden ketjuttaminen

Sähköisen asioinnin kautta tapahtuvassa tunnistamisessa ei voida koskaan täysin varmistua siitä, kuka tunnistustapahtuman tekee, vaan aina piilee riski siitä, että tunnistusväline on päätynyt toisen käsiin. Ensitunnistamisen ketjuttaminen korostaa tätä ongelmaa, koska yhden tunnistusvälineen saamisella käsiinsä rikollinen voi hankkia useita uusia tunnistusvälineitä ilman, että uhri saa tätä tietoonsa.

Ensitunnistamisen ketjuttaminen on merkittävä haaste rikostorjunnallisesti ja jo nykyisellään esiintyy runsaasti tapauksia, joissa rikolliset ovat hyödyntäneet tunnistusvälineiden ketjutusta toistuvasti saatuaan haltuunsa uhrin tunnistusvälineen. Rikolliset toimijat ovat hankkineet ketjuttamisen kautta etenkin mobiilivarmenteita, minkä seurauksena osa tunnistusvälineiden tarjoajista on luopunut ainakin osittain ketjuttamisesta.

Hallituksen esityksessä on esitetty muutoksia, joiden seurauksena tunnistuslain piiriin jäävien välineiden osalta välineen haltijan olisi mahdollista kieltää yksittäisen tunnistusvälineen käyttö ketjuttamiseen. Lisäksi on esitetty, että ketjuttamisesta olisi aina ilmoitettava ketjuttamiseen käytetyn tunnistusvälineen tarjoajalle. Muutokset ovat kannatettavia ja niillä voidaan nähdä olevan ainakin periaatteellinen hyöty rikostorjunnallisesta näkökulmasta.

Poliisihallitus haluaa kuitenkin tuoda hallituksen esityksen jatkovalmistelua varten esiin, että ensitunnistamisen ketjuttamista koskevan sääntelyn pienellä jatkojalostamisella voitaisiin saavuttaa merkittävämpiä rikostorjunnallisia hyötyjä ja tehdä sähköisestä tunnistamisesta turvallisempaa.

Ensinnäkin ensitunnistamisen ketjuttamista koskeva kieltä tulisi kääntää päinvastaiseksi. Voidaan olettaa, että suurin osa tunnistusvälineen haltijoista ei käsitä, mistä ensitunnistamisen ketjuttamisessa ja siihen liittyvissä riskeissä on kyse, joten he eivät osaa ennakollisesti varautua tällaiseen riskiin tekemällä oma-aloitteisesti kieltä. Olisi turvallisempaa, jos lähtökohtana olisi se, ettei tunnistusvälinettä saa käyttää ensitunnistamiseen, jollei käyttäjä ole tätä nimenomaisesti erikseen sallinut ilmaistuaan ymmärtävänsä siihen liittyvät riskit. On myös huomioitava, että ensitunnistamisen ketjuttaminen on lähtökohtaisesti melko poikkeuksellinen toimenpide tunnistustapahtumien massassa. Ketjuttamista ei olla tehty todennäköisesti kertaakaan suurimalla osalla nykyisin käytössä olevilla tunnistusvälineistä, joten ehdotettua rajoitusta ei voida pitää kohtuuttomana rasitteena tunnistusvälineen käyttökokemukselle suhteessa muutoksella saavutettavaan rikostorjunnalliseen hyötyyn.

Toinen ketjuttamista koskeva kehitysehdotus liittyy ketjuttamisesta ilmoittamiseen. Hallituksen esityksen luonnoksessa on asetettu tunnistustapahtuman vastaanottajalle velvollisuus ilmoittaa ensitunnistamisen ketjuttamisesta tunnistamisessa käytetyn tunnistusvälineen tarjoajalle. Tämä on tarpeellinen toimenpide, jonka potentiaalisia hyötyjä ei ole esitetyssä sääntelyssä ulosmitattu täysimääräisesti. Ensitunnistamisen ketjuttamiseen käytetyn tunnistusvälineen tarjoajalla ei ole todellisuudessa mitään keinoja arvioida sitä, onko tunnistustapahtuma tehty välineen haltijan toimesta vai jonkun toisen henkilön toimesta rikollisessa mielessä. Ainoa taho, joka voi ottaa kantaa siihen, onko tunnistustapahtuma tehty välineen haltijan toimesta, on välineen haltija itse. Tästä syystä olisikin ensiarvoisen tärkeää, että käytetyn tunnistusvälineen tarjoajalle asetetaan velvollisuus ilmoittaa välineen haltijalle tapahtuneesta ensitunnistamisen ketjuttamisesta. Tällä tavoin välineen haltija voisi puuttua välittömästi ketjuttamiseen, joka ei ole tapahtunut hänen omasta toimestaan. Ilmoituksen tulisi sisältää vähintään tiedot siitä, milloin välinettä on käytetty, minkä toimijan palveluun sitä on käytetty ja millä tavoin käyttäjä saa estettyä väärinkäytön jatkumisen.

Esitetyn sääntelyn pitäisi olla mahdollista tunnistuslain osalta, joka esitetyn muutoksen seurauksena on käytännössä puhtaasti kansallista sääntelyä.

Poliisihallitus haluaa kiinnittää huomiota siihen, että hallituksen esityksen luonnos vaikuttaa jättävän kokonaan sääntelyn ulkopuolelle sen, miten ketjuttamista koskevia rajoituksia voidaan soveltaa eurooppalaisen digitaalisen identiteetin lompakon osalta. Yhtäältä toisen välineen ketjuttaminen lompakon myöntämiseksi ja toisaalta lompakon ketjuttaminen toisen välineen myöntämiseksi jää nyt esitettyjen sääntelytoimien ulkopuolelle. Jatkovalmistelussa olisi syytä huolehtia siitä, että lompakkoja koskee vastaavat vaatimukset ensitunnistamisen ketjuttamisen osalta, jotta rikollisille toimijoille ei avata uutta välinettä rikosten tehtailuun.

Eurooppalainen digitaalisen identiteetin lompakko

Käyttöönotettavan lompakkoratkaisun vaikutuksia on vaikea arvioida, koska monet siihen liittyvät käytännön kysymykset jäävät avoimeksi tämän hallituksen esityksen pohjalta. Tämä on toki luonnollista, koska eurooppalainen digitaalisen identiteetin lompakko perustuu eIDAS-asetukseen, joka on kansallisesti suoraan sovellettavaa sääntelyä ja kansallinen sääntely vain täydentää asetusta lähinnä viranomaisten vastuiden osalta.

Lopullisten vaikutusarvioiden tekeminen on haastavaa myös sen takia, että kaikkia eIDAS-asetusta koskevia täytäntöönpanosäädöksiä ei ole vielä annettu eikä kaikki yksityiskohdat lompakon käyttöönottoon ja käyttöön liittyen ole käytettävissä. Poliisihallituksen tiedossa ei ole, miten lompakko voidaan ottaa käyttöön, miten hakijan henkilöllisyys varmistetaan käyttöönoton yhteydessä, kuinka monta samanaikaista lompakkoa käyttäjällä voi olla tai sisältyykö lompakkoon joitain mekanismeja, joilla varmistetaan, ettei se ole käyttöönoton jälkeen päätynyt väärän henkilön käsiin.

Poliisihallitus korostaa, että lompakon toteutuksessa on rikosten ehkäisemisen näkökulmasta tärkeää, että lompakon käyttöönottoprosessi suunnitellaan mahdollisimman turvalliseksi siten, ettei lompakkoa ole mahdollista hankkia toisen henkilöllisyydellä. Tämä edellyttää täsmällisyyttä erityisesti ensitunnistamiseen ja varsinkin ensitunnistamisen ketjuttamiseen liittyvien kysymysten osalta. Kansallisesti olisi syytä säännellä siitä, että ensitunnistamiseen käytetyn passin tai henkilökortin voimassaolo tulisi tarkistaa aina poliisin rekisteristä vastaavalla tavalla kuin hallituksen esityksessä on esitetty uutta velvollisuutta tunnistamislain puolelle.

Luonnollisen henkilön tunnistetiedot

Lompakossa luonnollisen henkilön pakollisia tunnistetietoja ovat henkilön nykyinen etunimi, nykyinen sukunimi, syntymäaika ja -paikka sekä kansallisuus. Pakollisten henkilötietojen määrä on henkilön yksilöimisen näkökulmasta valitettavan kapeat. Suomessa, puhumattakaan huomattavasti väkirikkaammista maista, on useita henkilöitä, joilla nimi, syntymäaika - ja paikka ovat identtiset. Tämä pakollisten tietojen luettelo tulee suoraan EU-sääntelystä, joten siihen ei ole mahdollista vaikuttaa kansallisella sääntelyllä.

Se, mihin olisi kuitenkin syytä kiinnittää huomiota kansallisessa sääntelyssä, on se mitä VTJ:n tietokenttää on tarkoitus käyttää ilmaisemaan henkilön syntymäpaikkaa. Suomessa on perinteisesti käytetty syntymäpaikkaa ilmaisevana tietona äidin synnytyksen hetkistä kotikuntaa eli syntymäkotikuntaa. Varsinaista syntymäpaikkaa ei merkitä VTJ:lle, jos henkilö ei ole syntynyt ulkomailla. Henkilö voi olla kuitenkin syntynyt täysin eri paikassa ja eri maassa, kuin henkilön syntymäkotikunta on. Passien osalta syntymäkotikunnan ja ulkomaisen syntymäpaikan osalta aiheutuu toisinaan haasteita, koska osalla hakijoista on molemmat. Sekaannusta aiheutuu etenkin silloin, kun kyseessä on kaksoiskansalainen, jonka kansalaisuus perustuu nimenomaan syntymäpaikkaan.

Digitaalisen identiteetin lompakon käyttöönoton ikäraja

Käytännössä ainoa lompakon käyttöönottoa koskeva säännös, joka hallituksen esitykseen on sisällytetty, koskee jäsenvaltioiden kansallisen harkinnan puitteissa olevaa käyttöönoton alaikärajaa. Poliisihallituksen näkökulmasta hallituksen esityksen luonnoksessa esitetty 13-vuoden ikäraja on liian alhainen ja tulee johtamaan identiteettivarkauksien ja petosrikollisuuden määrän kasvuun ja osaltaan yleisen luottamuksen laskuun suhteessa sähköiseen asiointiin.

Hallituksen esityksessä esitetty ikäraja koskeva sääntely muodostaa hyvin merkittävän poikkeuksen suhteessa voimassa olevaan lainsäädäntöön. Tällä hetkellä alaikäisen ei ole mahdollista saada lainkaan sähköistä tunnistamisvälinettä ilman huoltajan suostumusta. Alaikäisten asiointimahdollisuuksiin liittyviä puutteita on kritisoitu lähinnä sosiaali- ja terveysalan toimijoiden sekä koulutussektorin toimesta.

Lainsäädännöllisesti alle 18-vuotiaiden ja varsinkin alle 15-vuotiaisen lapsien kykyä tehdä itsenäisesti oikeustoimia on rajoitettu merkittävästi. Rajoittamalla alaikäisen oikeutta tehdä oikeustoimia pyritään suojelemaan häntä taloudellisilta ja muilta riskeiltä, jotka liittyvät oikeustoimen sitovuuteen. Oikeustoimet ovat tahdonilmauksia, joilla perustetaan, muutetaan tai kumotaan oikeuksia ja velvollisuuksia, esimerkiksi sopimukset.

Alaikäisten puhevaltaa viranomaisasiointinnissa säännellään yleisellä tasolla hallintolaissa, jonka mukaan vajaavaltaisen puolesta käyttää puhevaltaa hänen edunvalvojansa, huoltajansa tai muu laillinen edustajansa. Vajaavaltaisella on kuitenkin oikeus käyttää yksinään puhevaltaa asiassa, joka koskee hänen hallitsemaansa tuloa tai varallisuutta. Viisi-toista vuotta täyttäneellä alaikäisellä ja hänen huoltajallaan tai muulla laillisella edustajallaan on kummallakin oikeus erikseen käyttää puhevaltaa asiassa, joka koskee alaikäisen henkilöä taikka henkilökohtaista etua tai oikeutta.

Eräissä erityislaeissa on perustellusta syystä poikettu näistä yleisistä lähtökohdista. Yleensä poikkeukset muodostuvat suhteessa siihen, että alaikäinen on oikeutettu käyttämään puhevaltaa rinnakkain huoltajan kanssa eräissä tilanteissa ennen 15 vuoden ikään. Harvemmassa ovat poikkeukset, joissa alaikäiselle olisi myönnetty itsenäistä oikeutta tehdä oikeustoimia tai käyttää puhevaltaa ennen 15 -vuoden ikärajaa. Näistä löytyy joitakin rajattuja esimerkkejä lähinnä terveydenhuoltoon ja opetustoimeen liittyvistä säännöksistä. Kokonaisuutena kuitenkin on erittäin poikkeuksellista, että ylipäätään alle 18-vuotiaalla on oikeus tehdä oikeustoimia itsenäisesti.

Sähköisen tunnistamisvälineen kuten eurooppalaisen digitaalisen lompakon käyttöönotossa on kyse oikeustoimesta, jolla käyttäjä sitoutuu noudattamaan välineen käyttöehtoja ja vastaamaan välineen väärinkäytöstä seuraavista seuraamuksista. Henkilön kyky ymmärtää mikä sähköisen tunnistamisen väline on, ja mitä siihen liittyvät velvoitteet tarkoittavat, riippuu huomattavalla tavalla hänen kehitysasteestaan. Alaikäisen kyky ymmärtää ja hahmottaa monimutkaisia asioita ja asioiden kausaaliketjuja kehittyy yleensä iän karttuessa.

Alaikäisen voi olla haastavaa hahmottaa esimerkiksi sitä, että sähköinen tunnustusväline väärin käsiin joutuessaan mahdollistaa toisen lukuun tehtävän petosrikollisuuden. Jos välinettä ei ole ilmoitettu kadonneeksi on välineen haltija vastuussa tehdyistä oikeustoimista. Puhuttaessa vastuukysymyksistä voidaan hakea jotakin analogiaa esimerkiksi rikosoikeudellisen vastuun 15-vuoden ikäraja. Sääntelyssä on lähdetty siitä olettamasta, että 15-vuotta täyttänyt on riittävän kypsä ymmärtämään tekojensa kausaaliketjuja ja niistä seuraavaa vastuuta. Puhuttaessa sähköisestä tunnistamisvälineestä, voi käyttäjän olla jopa huomattavasti haastavampaa ymmärtää siihen liittyviä vastuita itsenäisesti. Tätä vielä korostaa entisestään se, että sähköisen tunnistusvälineen tarjoajan ei tarvitse tehdä hakijaa tietoiseksi välineen käyttöehdoista ennen myöntämistä, vaan riittää, että hakijalle osoitetaan, mistä esim. verkkosivuilta käyttöehdot ovat luettavissa. Lisäksi rikosoikeudellisen vastuun ikärajaan liittyen voi tulla kysymykseen myös tilanteet, joissa sähköistä välinettä pyritään käyttämään erilaisten oikeustoimien tekemisen toisinaan myös petollisessa tarkoituksessa.

Mikäli jatkovalmistelussa päädytään pitämään hallituksen esityksen luonnoksessa nyt oleva 13-vuoden ikäraja, olisi hallituksen esitykseen tuotava kattavasti esiin myös valittuun ikärajaan liittyvät riskit rikollisuuden kasvusta. Voidaan olettaa, että lapset ovat huomattavasti alttiimpi manipulaatiolle, jolla henkilö taivutetaan hakemaan itsenäisesti lompakko ja luovuttamaan se toiselle henkilölle, joka korvausta vastaan tai korvauksetta. Lapsen on hankala ymmärtää tähän liittyvät riskit ja koska väline voidaan myöntää ilman huoltajan osallistumista, on todennäköistä, että väline jää rikollisen toimijan haltuun pitkäksi aikaa. Välinettä voidaan pyrkiä hyväksikäyttämään Suomessa tai toisessa lompakon hyväksyvässä valtiossa joko heti tai mahdollisesti vasta pidemmän ajan päästä, jolloin lompakko mahdollistaa kattavammin erilaisten oikeustoimien tekemisen. Hallituksen esityksen perusteella ei pysty päättämään, onko lompakkoon suunniteltu jonkinlaisia välineitä, jolla voidaan varmistua siitä, että lompakko todella on oikean käyttäjän hallussa eikä mahdollisesti vuosikausia jonkun rikollisen tahon hallussa, kun alaikäinen käyttäjä ei osaa, ymmärrä tai uskalla itse ilmoittaa, että väline on toisen henkilön hallussa.

Lisäksi olisi toivottavaa, että hallituksen esityksen perustelut nojautuisivat valittua ikärajaa koskeviin puolesta ja vastaan olevista argumenteista eikä nyt esitetyllä tavalla yleiseen viittaukseen tietosuojalain 5 §:ään. Valintaa on perusteltu väitteellä, että tietosuojalain 5 §:n johdosta yksityiset voisivat myöntää lompakoita 13-vuotiaille ilman huoltajan suostumusta, minkä vuoksi myös valtion myöntämän lompakon ikärajaksi tulisi asettaa 13-vuotta.

Lisäksi päättelyketju, joka hallituksen esityksessä on esitetty tietosuojalain 5 §:stä on on-tuva. Mainitusta säännöksestä ei hallituksen esityksen luonnoksessa väitetyllä tavalla johdu, että yksityiset toimijat voisivat tarjota lompakkoja 13-vuotiaille ilman huoltajan suostumusta, koska kyseisellä säännöksellä ei ole tarkoitus säännellä alaikäisen oikeus-toimikelpoisuudesta. Säännös koskee vain ja ainoastaan sitä, että yksityiset toimijat saa-vat käsitellä edes henkilön perushenkilötietoja, kuten nimeä 13-vuotta täyttäneen henki-lön omalla suostumuksella. Säännöksestä ei johdu, että kolmetoistavuotias voisi tehdä pätevästi ankaraa vastuuta sisältävän oikeustoimen, kuten sähköiseen asiointiin tarkoite-tun lompakon käyttöönoton. Jos yksityinen toimija ryhtyisi oikeustoimeen alaikäisen kanssa kyseisen säännöksen perusteella, oikeustoimi olisi mitätön, koska henkilö ei ole ollut oikeustoimikelpoinen.

Lisäksi hallituksen esityksen luonnoksessa on jätetty kokonaan huomioimatta se, että käyttöönoton ikärajasta voidaan säännellä tässä hallituksen esityksessä myös yksityistä sektoria koskevasti eikä sääntelyssä ole tarve siis nojata olemassa olevaan sääntelyyn. Näin ollen käsillä olevaan hallituksen esityksessä tulisi perustella yksityiskohtaisesti se mitä hyötyjä ja haittoja on sillä, että tietty ikäraja valitaan. Jatkovalmistelussa tulisi myös tehdä kansainvälinen vertailu siitä, mille tasolle kussakin EU-jäsenvaltiossa sähköisen tunnistamisen välineiden itsenäisen hakemisen alaikäraja on asetettu.

Digitaalisen henkilöllisyystodistuksen käyttöönotto

Hallituksen esityksen luonnoksessa huomio kiinnittyy siihen, että digitaalisen henkilöl-li-syystodistuksen myöntäminen vaikuttaisi sisältävän ylimääräistä byrokratiaa päällekkäi-sen päätöksenteon muodossa. On esitetty, että poliisi myöntää digitaalisen henkilöl-li-syystodistuksen sillä perusteella, että henkilöllä on Suomen viranomaisen myöntämä passi tai henkilökortti. Lisäksi on esitetty, että DVV myöntää myönnetyn digitaalisen hen-kilöllisyystodistuksena käytetyn sähköisen attribuuttitodistuksen. Hakemusmenettely ja päätöksenteko edellyttävät aina lähtökohtaisesti hallintolain menettelysäännösten mu-kaista hallintoprosessia. Kokonaistaloudellisesti on edullisempaa, jos luodaan sääntely-malli, joka sisältää mahdollisimman vähän byrokratiaa. Digitaalinen henkilöllisyystodistus on lompakon käyttöön ottaneelle tietyn tyyppisen passin tai henkilökortin omaavalle hen-kilölle ilman minkäänlaista päätösharkintaa myönnettävä lupa-asiakirja.

Poliisihallituksen näkökulmasta olisi toivottavampaa, että digitaalisen henkilöllisyystodis-tuksen prosessia lähestyttäisiin enemmän vastaavasta näkökulmasta kuin edellisen digi-taalisen henkilöllisyystodistuksen hankkeen yhteydessä. Eli oikeus digitaalisen henkilöl-li-syystodistuksen käyttöönottoon syntyisi suoraan passin tai henkilökortin myöntöpäätök-sessä. Tällöin digitaalinen henkilöllisyystodistus olisi ikään kuin passin tai henkilökortin lisäominaisuus, joka sisältyy varsinaisen asiakirjan myöntöpäätökseen. Oikeus ottaa di-gitaalinen henkilöllisyystodistus käyttöön, olisi sidottu fyysisen asiakirjan voimassaoloon eikä varsinaisesti passin tai henkilökortin myöntöpäätökseen, jolloin jo myönnettyjen passien ja henkilökorttien osalta ei edellytettäisi erillistä jälkikäteistä digitaalisen henkilöl-li-syystodistuksen myöntöpäätöstä.

Tällä tavoin välttyttäisiin viranomaisiin kohdistusvalta moninkertaiselta hallinnolliselta taa-kalta ja malli olisi johdonmukainen sen ajatuksen kanssa, että digitaalinen henkilöllisyys-todistus on fyysisen passin tai henkilökortin digitaalinen ilmentymä. Lisäksi Poliisihallituk-sen tietojärjestelmätoteutus on rakennettu tältä pohjalta ja uuden hakemukseen ja pää-töksentekoon perustuvan mallin toteuttaminen edellyttää tarpeettomia kustannuksia tie-tojärjestelmien kehitykseen.

Lisäksi digitaalisen henkilöllisyystodistuksen käyttöönottoon liittyen hallituksen esityksen jatkovalmistelussa olisi toivottavaa ottaa kantaa siihen, voiko henkilöllä olla käytössään useampi digitaalinen henkilöllisyystodistus samanaikaisesti. Poliisihallitus pitää erittäin tärkeänä, että samanaikaisten kopioiden määrä on erittäin rajallinen. Digitaalinen henki-löllisyystodistus on ensisijaisesti käyntiasiointiin käytettävä väline ja sitä voi käyttää aino-astaan yksi henkilö yhdessä fyysisessä paikassa kerrallaan. Useamman kopion käyt-töönotto mahdollistaisi samanaikaiset väärinkäyttöyritykset eri sijainneissa. Käyttöä ei ole myöskään mahdollista valvoa, koska viranomaisella ei ole pääsyä lompakon ja sen sisältämien attribuuttien käyttötietoihin. Vastaavalla tavalla fyysisiä asiakirjojakaan ei ole mahdollista monistaa hakijan omilla toimilla. Toivottavinta olisi, että henkilöllä voisi olla ainoastaan yksi digitaalinen henkilöllisyystodistus käytössään yhdellä kertaa.

Eräs käyttöönottoon liittyvä seikka koskee myös käyttöönoton yhteydessä tapahtuvaa fyysisen asiakirjan lukemista. Sen lisäksi, että asiakirjan aitous ja eheys tarkistetaan si-run avulla, tulee myöntömenettelyssä varmistua siitä, että kyseinen asiakirja on voi-massa oleva. Muussa tapauksessa varastetuksi tai kadonneeksi ilmoitettua tai mitätöityä asiakirjaa on mahdollista käyttää digitaalisen henkilöllisyystodistuksen käyttöönottoon. Voimassaoloa ei ole mahdollista tarkistaa käytännössä kuin poliisin passirekisterin tai henkilökorttirekisterin tiedoista. Jatkovalmistelussa olisi syytä huolehdittava siitä, että asiakirjan voimassaolo tarkistetaan digitaalisen henkilöllisyystodistuksen käyttöönoton yhteydessä.

Digitaalisen henkilöllisyystodistuksen tietosisältö

Hallituksen esityksen jatkovalmistelussa tulisi täsmentää digitaalisen henkilöllisyystodis-tuksen tietosisältöä koskevaa 4 §:ää. Pykälän 1 momentin 9 kohdassa mainitaan todis-tuksen yksilöivä tunniste ottamatta sen täsmällisemmin kantaa siihen, miten tunniste muodostetaan ja mikä sen käyttötarkoitus on. Digitaalisen henkilöllisyystodistuksen tur-vallisen käytön ja tunnistustapahtuman jälkikäteisen todentamisen näkökulmasta, on olennaista, että asiakirjaa esitettäessä tunnistajalle välitetään nimenomaan sellainen tieto, jonka avulla voidaan määritellä, onko kyseinen luvan ilmentymä ollut voimassa väi-tettynä tunnistamisajankohtana ja mistä laitteesta lupa on esitetty.

Asiaa voitaneen selventää esimerkin kautta. Henkilö ottaa käyttöönsä digitaalisen henki-löllisyystodistuksen. Osoituksena kyseisestä digitaalisesta henkilöllisyystodistuksesta henkilöllä ehtii olla useita attribuuttitodistuksia. Lisäksi, jos lainsäädäntö sallii esimerkiksi kahden digitaalisen henkilöllisyystodistuksen samanaikaisen voimassaolon, on syntyvien attribuuttitodistusten lukumäärä lähtökohtaisesti kaksinkertainen. Kun henkilö esittää henkilöllisyytensä asiointitilanteessa esimerkiksi pankissa, on pankin tietyissä tilanteissa

talletettava esitetyn tunnistamisasiakirjan numero. Jotta tunnistamistapahtuman ajankohta ja digitaalisen henkilöllisyystodistuksen esittämiseen käytetty mobiililaitte voitaisiin varmentaa jälkikäteisesti olisi olennaista, että esitetty digitaalisen henkilöllisyystodistuksen lupanumero eroaa sen mukaan mikä attribuuttitodistus on ollut käytössä, kun lupaa on esitetty. Eli digitaalisella henkilöllisyystodistuksella ei tulisi olla kiinteää lupanumeroa, vaan sen tulisi olla sidottu kulloinkin voimassa olevaan sähköiseen attribuuttitodistukseen.

Digitaalisen henkilöllisyystodistusten tietojen maantieteellinen sijainti

Hallituksen esitys ei ota millään tavalla kantaa siihen, millä maantieteellisellä alueella viranomaiset voivat käsitellä digitaalisen henkilöllisyystodistuksen tietoja. Näin ollen tiedon vapaan liikkuvuuden periaatteesta seuraa, että tietojen käsittely on mahdollista EU- ja ETA-alueella. Lainsäädännön johdonmukaisuuden vuoksi tulisi kuitenkin huomioida se, että sekä passilaista että henkilökorttilaista löytyy säännökset siitä, että asiakirjojen yksilöinnin ja laaduntarkastamisen tulee tapahtua Suomen rajojen sisäpuolella.

Säännös on lisätty aikoinaan passilakiin perustuslakivaliokunnan aloitteesta. Hallintovaliokunnan mietinnössä HaVM 4/2013vp todetaan, että *passilain 29 §:n mukainen passi-rekisteri on huomattavan laaja, sisäisen turvallisuuden kannalta merkittävä tietokanta, joka sisältää Suomen kansalaisten henkilöllisyyttä koskevia tietoja valokuvineen ja sormenjälkitietoineen ja johon voidaan katsoa kohdistuvan erityisen korkeita tietoturva vaatimuksia. Tietojen luonne on myös yksittäisessä tapauksessa hyvin merkityksellinen ja siten erityisen suojan tarpeessa. Nämä ovat valiokunnan mielestä sellaisia turvallisuuteen liittyviä syitä, että järjestelyissä tarvitaan normaalia korkeampaa luotettavuutta. Tämän vuoksi valiokunnan mielestä esimerkiksi yrityksestä ennen palveluntuottamista koskevan sopimuksen solmimista tehty luotettavuusarviointi ja säädetty velvollisuus huolehtia asianmukaisesti asiakirjaturvallisuudesta ja tietosuojasta eivät yksin riitä, vaan on tärkeää, että passin ja sen sirun yksilöinti ja siihen liittyvä passin laadun ja oikeasisältöisyyden tarkastaminen tapahtuu Suomessa ja että yksilöintitietoja ei siirretä Suomen rajojen ulkopuolelle.*

Digitaalinen henkilöllisyystodistus on passin tai henkilökortin digitaalinen ilmentymä, joka pitää sisällään pääasiallisesti samat tiedot kuin fyysinen asiakirja. Digitaalinen henkilöllisyystodistus käyttää henkilötietoja poliisin rekisterin kautta, jota koskee erityisen korkeat tietoturva vaatimukset. Digitaalisen henkilöllisyystodistuksen käyttöönotto ja sähköisen attribuuttitodistuksen myöntäminen rinnastuvat hyvin pitkälti fyysisen lupa-asiakirjan yksilöintiin. Mikäli digitaalisen henkilöllisyystodistuksen osalta mahdollistetaan laajempi maantieteellinen alue, jolla tietoja saa käsitellä, tehdään passilain ja henkilökorttilain tietojen suojaamista koskeva sääntely tyhjäksi. Ei ole johdonmukaista sääntelyä, jos saman tiedon käsittely kielletään yhtäällä, koska siihen sisältyy merkittäviä turvallisuusriskejä, ja toisaalla tiedon käsittely sallitaan vapaasti.

Digitaalinen henkilöllisyystodistuksen vaatima lompakko

Hallituksen esityksen jatkovalmistelussa olisi syytä kiinnittää huomiota siihen, että sääntelyssä tulisi selkeästi esiin se, mihin eurooppalaiseen digitaalisen identiteetin lompakkoon digitaalinen henkilöllisyystodistus voidaan ottaa käyttöön. Lompakoista säännellään eIDAS-asetuksessa ja jokaiselle jäsenvaltiolle on asetettu velvoite huolehtia siitä, että valtion alueella lasketaan liikkeelle asetuksen tarkoittama lompakko joko valtion tai yksityisen toimijan aloitteesta. Lompakoita, jotka tulee hyväksyä Suomessa tulee olemaan siis useita kymmeniä.

Digitaalinen henkilöllisyystodistus hyödyntää tietomassaa, joka sisältää noin 4,5 miljoonaa Suomalaista koskevat yksityiskohtaiset henkilötiedot. Samaan tapaan kuin tietojenkäsittelyn maantieteellisen käsittelyn osalta, olisi syytä säännellä tarkkarajaisesti siitä, mihin lompakoihin digitaalinen henkilöllisyystodistus voidaan ladata. Poliisihallitus katsoo, että sisäisen turvallisuuden ja yksilöiden henkilötietojen turvaamisen näkökulmasta paras vaihtoehto on se, että digitaalisen henkilöllisyystodistuksen käyttöönotto mahdollistetaan ainoastaan DVV:n liikkeelle laskemassa Suomen kansallisessa eurooppalaisessa digitaalisen identiteetin lompakossa.

Poliisihallitus pitää kestävämmänä tilannetta, jossa suomalainen henkilöllisyystodistus voitaisiin myöntää jonkin toisen valtion liikkeelle laskemaan lompakkoon. Kolmas vaihtoehto on sallia digitaalisen henkilöllisyystodistuksen tarjoaminen myös muihin Suomessa liikkeelle laskettuihin lompakoihin. Poliisihallitus ei pidä myöskään tätä vaihtoehtoa toivottavana siitäkin huolimatta, että lompakon liikkeelle laskeviin yrityksiin kohdistetaan ehdotetun sääntelyn mukaan tiukkoja valvontatoimia. Fyysisten tunnistusvälineiden tarjoaminen ja valmistaminen on selkeästi viranomaistehtävä, joten myös näiden välineiden digitaalisten ilmentymien alustan tulisi vastaavalla tavalla olla viranomaisten liikkeelle laskema.

Jos säädöksen jatkovalmistelussa päädytään täsmentämään asiaa Poliisihallituksen näkemyksen vastaisesti, tulee huomioida, että sääntely muodostaa selkeän kokonaisuuden myös muilta osin. Onko käyttöönottoa koskeva sääntely riittävä etenkin fyysisen asiakirjan lukemisen osalta. Mahdollisten tietojen käsittelyä koskevien alueellisten rajoitusten noudattamista koskevien vaatimusten valvonta ja valvonnan resurssointi olisi myös huomioitava.

Digitaalisen henkilöllisyystodistuksen käyttö

Digitaalisen henkilöllisyystodistuksen osalta tulisi sääntelyyn lisätä säännökset, jotka mahdollistavat sen käytön passiin ja henkilökorttiin rinnastettavana henkilöllisyyden osoittamisen välineenä. Ensinnäkin tunnistuslakiin tulisi mainita siitä, että myös digitaalinen henkilöllisyystodistus käy ensitunnistamisen välineenä. Passeista ja henkilökorteista annettuun valtioneuvoston asetuksen 1 §:ään tulisi lisätä säännös siitä, että digitaalista henkilöllisyystodistusta voi käyttää tunnistamisasiakirjana passia ja henkilökorttia haettaessa.

Lisäksi tulisi varmistua siitä, että mikäli toisaalla lainsäädännössä todetaan, että henkilöllisyyden osoittamiseen on mahdollista vain tietyillä asiakirjoilla tulisi lakia muuttaa siten, että henkilöllisyyden osoittaminen on mahdollista myös digitaalisella henkilöllisyystodistuksella.

Viittaussäännökset

Hallituksen esityksen jatkovalmistelussa on syytä käydä läpi vielä eri lakien viittaussäännökset tunnistuslakiin ja eIDAS-lakiin. Kokonaisuus on monimutkainen, kun osa ole-massa olevasta sääntelystä siirretään toiseen lakiin.

Ensinnäkin, mahdollistaako nykyiset eri lakeihin sisältyvät viittaussäännökset lompakon kautta tapahtuvan asiointin viranomaisasiointiin riittävän selkeästi. Esimerkiksi voidaan ottaa passilaki, jonka 6 § 4 momentin mukaan "Sähköinen asiointi edellyttää vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa (617/2009)". tarkoitettua tunnistusvälinettä. Koska lompakosta säännellään eIDAS-laissa, ei se täytä passilain edellytystä. Toki eIDAS-asetus on suoraan sovellettavaa sääntelyä ja se velvoittaa viranomaisia hyväksymään välineen, mutta lainsäädännön selkeyden ja täsmällisyyden vuoksi voitaisiin harkita viittaussäännösten lisäämistä myös eIDAS-lain mukaiseen lompakkoon. Tämä ei olisi lähtökohtaisesti suuri työ, koska hallituksen esityksen luonnoksen sivulla 135 on esitetty muut liitelait, joiden osalta on tarkoitus korjata viittaussäännökset, kun tunnistuslain nimi päivittyy.

Toinen kysymys liittyy laissa väestötietojärjestelmästä ja digi- ja väestötietoviraston varmennepalveluista organisaatiovarmenteen ja kansalaisvarmenteen osalta viitataan tunnistuslakiin. Kun lainsäädännön yhteydessä kuitenkin luottamuspalveluja koskeva sääntely siirretään tunnistuslaista osaksi eIDAS-lakia, olisiko laissa väestötietojärjestelmästä ja digi- ja väestötietoviraston varmennepalveluista esiintyviä viittaussäännöksiä korjattava tämän takia. Lisäksi kansalaisvarmenteessa on kyse ainoasta eIDAS notifioidusta välineestä ja kaikki rajat ylittävää asiointia koskeva sääntely oli tarkoitus siirtää eIDAS-lakiin.

Henkilötietojen käsittelyä koskeva sääntely

Hankkeen jatkovalmistelussa tulisi huomioida, että laki henkilötietojen käsittelystä poliisi-toimessa on sopusoinnussa nyt esitettyjen lakimuutosten kanssa. Se tulee ainakin varmistaa, että poliisin tietojenluovuttamista ja tiedonsaantia koskevat säännökset kattavat kaikki uudet tehtävät riittävällä tavalla.

Juhani Ruutu, Ylitarkastaja

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Poliisi 28.08.2025 klo 19:43. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Liitteet

-

Jakelu

VM/kirjaamo

Tiedoksi

POHA esikunta

Poliisihallitus

Vuorimiehentie 3, PL 1000, 02151 Espoo

kirjaamo.poliisihallitus@poliisi.fi

Puhelin +358 295 480 181, Faksi +358 295 411 780, poliisi.fi