

Asia: VN/17113/2022

Lausuntopyyntö lakiluonnoksesta henkilötunnuksen käsittelyä koskevien säännösten täsmentämisestä

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Esitys on sinänsä kannatettava, mutta kaipaa tarkennuksia

FA kannattaa esityksen peruseriaatetta, mutta kaipaa tarkennusta pankkien sulkupalvelun ja vahvan sähköisen tunnistamisen menettelyiden osalta.

Olisi erittäin toivottavaa, että käynnissä olevassa valtion digitaalisen identiteetin hankkeessa kehitettäisiin toiminnallisuus, jonka avulla valtion sähköistä henkilöllisyystodistusta voitaisiin jatkossa käyttää henkilöllisyyden todentamiseen myös puhelinasioinnissa.

Ehdotuksen ulottuvuus

FA kannattaa ehdotuksessa omaksuttua peruslinjaa, jonka mukaan pelkkää henkilötunnusta tai henkilötunnuksen ja nimen yhdistelmää ei saa käyttää henkilöllisyyden todentamiseen. Omaksuttu linja noudattaa nykyistä Tietosuojavaltuutetun ohjeistusta.

Laajempi henkilötunnuksen käytön kieltö olisi kohtuutonta ottaen huomioon sen esityksessäkin mainittu vakiintunut laaja käyttö, joka mahdollistaa myös sujuvan ja virheettömän tietojen siirtämisen organisaatioiden välillä.

Ehdotetussa laajuudessaankin kiello kuitenkin tuottaa ilman lisäselvennyksiä ongelmia pankkipalveluiden sulkupalveluissa ja mahdollisesti myös sähköisen tunnistamisen lainsäädännön noudattamisessa.

Henkilötunnuksen ja nimen käyttö sulkupalvelussa

Pankkien sulkupalvelun tarkoituksena on mahdollistaa palvelujen nopea passivointi silloin, kun asiakkaan maksukortti tai pankkitunnukset ovat kadoksissa, varastettu tai asiakas on joutunut tietojenkalastelun kohteeksi. Tällaisessa tilanteessa asiakkaan taloudellisen aseman turvaamiseksi on ehdottoman tärkeää, että palvelut voidaan passivoida nopeasti, koska rikolliset voivat olla parhaillaan tekemässä asiakkaan varojen siirtoja verkkopankissa. Aikaa ei siis ole käytettävissä ylimääräisten kysymysten kysymiseen asiakkaalta.

Ympäri vuorokauden toimivissa sulkupalveluissa käytetään myös alihankkijoita, joille halutaan tietosuojasyistä antaa vain erittäin rajattu pääsy pankin asiakasjärjestelmiin. Sulkupalvelulla ei näin ollen ole käytettävissään lisätietoja, joilla ne pystyisivät asiakkaan henkilöllisyyttä varmistamaan. Pankkien normaalissa puhelinpalvelussa voidaan poikkeustapauksissa, jos asiakkaan sähköinen tunnistaminen puhelimesta ei onnistu, henkilöllisyyden varmistamiseksi kysyä laajastikin kysymyksiä henkilön asiointiin liittyen. Tätä mahdollisuutta ei sulkupalvelussa voida käyttää edellä mainitun aikapaineen ja toisaalta alihankkijoiden niukemman tietomäärän takia.

Henkilötunnus on pankkien järjestelmissä yleisesti avaimena käytetty yksilöivä tunniste. Se on myös tieto, jonka omaisuutensa kadottamisesta tai rikoksen kohteeksi joutumisesta hätäantunut henkilö nimensä ohella todennäköisesti muistaa, toisin kuin esim. pankin asiakasnumeron. Sen vuoksi yksilöinti ja palvelujen passivointi nimenomaan henkilötunnuksen avulla tulee olla sulkupalvelussa jatkossakin mahdollista.

Vaikka henkilötunnuksen ja nimen kysymistä ei pankeissa missään olosuhteissa pidetä henkilöllisyyden varmistamisena, vaan sulkutoimenpiteet tehdään käytännössä henkilön yksilöinnin perusteella, on vaarana, että ehdotetun 29 a § pykälän voidaan tulkita kieltävän myös kuvatun kaltaisen palvelujen passivoinnin.

Palvelun passivointi estää asiakkaalta kyseisen palvelun käytön siihen saakka, kunnes hän pystyy vahvasti tunnistautuneena joko sähköisesti tai käyntiasioinnissa todentamaan henkilöllisyytensä ja aktivoimaan palvelun takaisin käyttöön tai tarvittaessa tilaamaan sen uudestaan. Toisen puolesta tehdyllä passivoinnilla voi siis aiheuttaa haittaa palvelujen käyttäjälle. Tällainen haittatarkoituksessa tehty passivointi on kuitenkin äärimmäisen harvinaista ja myös vaikutuksiltaan varsin rajattua, joten henkilötunnuksen ja nimen perusteella tapahtuvan passivoinnin voidaan katsoa olevan varsin vähäriskistä. Sen sijaan passivoinnin myöhästymisestä tai tekemättä jäämisestä asiakkaalle

aiheutuva taloudellinen vahinko voi olla merkittävä ja tarkoittaa jopa kaiken varallisuuden menettämistä.

Tämän vuoksi on tärkeää, että ehdotettuun säädökseen tuodaan poikkeamismahdollisuus, jota voitaisiin käyttää henkilön välttämättömän taloudellisen (tai mahdollisesti muunkin henkilökohtaisen) edun turvaamiseksi.

Henkilötunnus ja nimi vahvassa sähköisessä tunnistamisessa

Tunnistamislain 42 § perusteella on Traficom antanut määräyksen 245890/03.04.05.00/2020, jossa määritellään sähköisellä tunnistustapahtumalla annettavat tiedot. Kyseisen määräyksen luvun 3 kohdan 12 mukaan tunnistamistapahtumalla Luottamusverkostossa tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa välitettävät vähimmäistiedot ovat: ”Pakolliset tiedot: 1) luonnollista henkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja henkilön syntymäaika;”.

Käytännössä asiointi sähköisen tunnistamisen jälkeen tapahtuu henkilötunnuksen ja nimen perusteella. Koska henkilötunnus itsessään sisältää syntymäajan, ei tapahtumalla annettavalla erillisellä syntymäaikatiedolla ole merkitystä lisävarmistuksen antajana eikä sitä FA:n käsityksen mukaan voida pitää henkilöllisyyden varmistamiseksi käyttökelpoisena muuna henkilöä koskevana tietona.

Esityksessä olisikin syytä todeta, että henkilötunnuksen ja nimen yhdistelmän avulla tapahtuva asiointi tunnustslain mukaisessa vahvassa sähköisessä tunnistamisessa on jatkossakin sallittua.

Henkilöllisyyden todentaminen puhelinasiointissa

Kuten esityksessäkin todetaan, on sähköiseen asiointiin saatavissa tunnistuslain mukaisia vahvan sähköisen tunnistamisen palveluita. Puhelinasiointiin ei tällaista palvelua sen sijaan ole yleisesti saatavissa, vaan esim. pankit ovat rakentaneet ko. toiminnallisuuden omiin järjestelmiinsä mahdollistaakseen riskittömän puhelinasioinnin.

Esimerkiksi viranomaisissa tai terveydenhuollossa tapahtuvaan puhelinasiointiin voi myös sisältyä riskejä, joiden takia vahva tunnistaminen olisi tarpeen silloin kun tehdään henkilön taloudelliseen tilanteeseen vaikuttavia toimenpiteitä tai annetaan henkilöä koskevia, tietosuojan piiriin kuuluvia tietoja.

Kuten FA on todennut jo lausunnossaan luonnoksesta hallituksen esitykseksi digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi, puhelinasioinnin toiminnallisuuden ulos rajaaminen on selkeä puute kyseisessä hankkeessa. Olisi erittäin toivottavaa, että hankkeessa kehitettäisiin myös toiminnallisuus, jonka avulla valtion sähköistä henkilöllisyystodistusta voitaisiin jatkossa käyttää henkilöllisyyden todentamiseen myös puhelinasioinnissa.

Terminologiasta

Henkilöiden erottelusta toisistaan ja asioivan henkilön henkilöllisyyden varmistamisesta eri lainsäädännössä ja puhekielessä käytetty terminologia on jonkin verran horjuvaa.

Esityksessä todetaan:” Pääasiassa henkilötunnusta käytetään henkilön yksiselitteiseen yksilöimiseen tietojärjestelmässä ja asiakirjoissa. Henkilötunnusta käytetään erityisesti silloin, kun pelkkä nimi ja syntymäaika eivät riitä erottamaan henkilöitä toisistaan. ... erityisesti viranomaisten järjestelmissä sekä yksityisen sektorin järjestelmissä, joissa henkilön yksiselitteinen yksilöiminen on tärkeää, käytetään yleisesti henkilötunnusta... Henkilötunnusta käytetään sen käyttötarkoituksen, henkilön yksiselitteisen yksilöinnin, lisäksi monissa tilanteissa myös henkilön tunnistamiseen asiointitilanteissa. Henkilöllisyyden varmistamis- tarkoituksessa henkilötunnusta tai henkilötunnuksen loppuosaa voidaan kysyä asiointissa salasanan kaltaisena tietona...”

Esityksen perusteluissa tunnistamista käytetään siis synonyymina henkilöllisyyden varmistamiselle. Varmistaminen vastannee pykälätekstissä käytettyä todentaminen-termiä.

Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (7.8.2009/617; tunnistuslaki) 2 §:ssä tarkoitetaan tunnistamisella henkilön yksilöintiä ja todentamista ”1) vahvalla sähköisellä tunnistamisella sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset;”

Laki rahanpesun ja terrorismin rahoittamisen ehkäisemisestä (28.6.2017/444; rahanpesulaki) 4 § määrittelee termit näin: ”6) tunnistamisella asiakkaan henkilöllisyyden selvittämistä asiakkaan toimittamien tietojen perusteella; 7) henkilöllisyyden todentamisella asiakkaan henkilöllisyyden varmistamista luotettavasta ja riippumattomasta lähteestä peräisin olevien asiakirjojen tai tietojen perusteella;”

Tietosuojalaissa ei ole määritelty yksilöintiä, tunnistamista tai todentamista. Ehdotetussa tietosuojalain 29 a §:ssä omaksuttu ”henkilöllisyyden todentaminen” on linjassa rahanpesulain kanssa ja myös tunnistuslain pohjalta ymmärrettävä.

FA toteaa, että on kuitenkin jonkin verran hämmentävää, että tunnistaminen-termiä käytetään suomalaisessa lainsäädännössä sekä rahanpesulain mukaisessa suppeassa, pelkästään henkilön yksilöintiä tarkoittavassa merkityksessä, että tunnistuslain mukaisesti laajana kattaen sekä yksilöinnin että henkilöllisyyden todentamisen.

FINANSSIALA RY

Hannu Ijäs

Kaarlela Teija-Liisa
Finanssiala ry - Johtaja Hannu Ijäs