

Asia: VN/10855/2024

Luonnos hallituksen esityksestä eduskunnalle sähköisestä tunnistamisesta, luottamuspalveluista ja eurooppalaisesta digitaalisesta identiteetistä annettua EU:n asetusta täydentäväksi lainsäädännöksi

Lausunnonantajan lausunto

Huomiot rajat ylittävän sähköisen tunnistamisen, sähköisten luottamuspalvelujen ja eurooppalaisen digitaalisen identiteetin kansallisesta sääntelystä:

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 voimakasta kasvua. Keskusrikospoliisi pitää hyvänä sitä, että verkkoasioinnissa pankkiasiointiin pohjautuva sähköinen tunnistautuminen korvautuu muilla luotettavilla tunnistautumisen menetelmillä. Nykyinen tilanne on ollut rikostorjunnallisesti riskialtis.

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 miljoo-nan euron edestä rahaa vuonna 2024. Vuonna 2023 määrä oli 76,9 miljoonaa euroa. Esitetyt luvut edustavat todennäköisesti vain osaa todellisista aiheutuneista vahingoista.

Samalla laajenee tunnistamispalveluiden tarjoaminen perinteisten pankkien ja viranomaisten ulkopuolelle erilaisille palveluntarjoajille. Rikosten ennalta estämisen, paljastamisen ja selvittämisen kannalta olennaista on tunnistamispalveluiden 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.

Poliisin toimivaltuudet estää varmenteen tai lompakon käyttö

Laki rajat ylittävästä sähköisestä tunnistamisesta, sähköisistä luottamuspalveluista ja eurooppalaisesta digitaalisesta identiteetistä 10 §, 16 §

Laki vahvasta sähköisestä tunnistamisesta 25 §

Keskusrikospoliisi kiinnitti luonnoksen osalta huomioita siihen, että väärinkäyttötilanteiden osalta kansallisessa täytäntöönpanolaissa ei ole arvioitu tai ehdoteta poliisille toimivaltuuksia antaa eurooppalaisen sähköisen identiteetin lompakon (EUDI) käyttöön liittyviä määräyksiä estää varmenteen tai lompakon käyttö rikosepäilyn tilanteessa. Ehdotuksen perusteella vaikuttaisi siltä, että väärinkäyttötilanteissa (esimerkiksi identiteettivarkaupauksissa) vain kohteella olevalla henkilöllä on mahdollisuus esittää käytön estämistä.

Vaihtoehtoisesti tunnistusvälineen tarjoaja voisi estää käytön, jos sen tietoon tulee, että joku muu kuin se, jolle tunnistusväline on myönnetty, käyttää sitä. Vaihtoehtoina estää tunnistuspalvelun käyttö on varmenteen peruuttaminen tai lompakon käytön estäminen. Tässä yhteydessä tulisi arvioida myös, että jos tunnistusvälineillä on avattu uusia tunnistusvälineitä, tulisiko ne pystyä peruuttamaan sulkemalla ensimmäinen tunnistusväline, joka oli menetetty. Vaihtoehtoisesti varmenteen peruuttamisella tulisi olla tämä sama vaikutus.

Lainalaisuusperiaatteen mukaan julkisen vallan käytön on perustuttava lakiin. Tällä hetkellä mikään poliisin pakkokeinolain mukaisista toimivaltuuksista ei vaikuta soveltuvan tällaisen EUDI väärinkäytön estävän määräyksen perusteeksi. Määräys varmenteen tai lompakon käytön estämiseksi voitaisiin ilmeisesti antaa EUDI palveluntarjoajalle tai DVV:lle. Ehdotuksen mukaan vaikuttaisi, että toiminta tällaisessa tilanteessa pohjautuisi pitkälti viranomaisten väliseen

yhteistyöhön, jossa poliisi voisi osaltaan olla aloitteellinen käytön estämiseksi, mutta ei poliisin osalta nimenomaiseen toimivaltuussäännökseen. eIDAS sääntelyssä on kansallisten viranomaisten toimivaltuudet jätetty tältä osin kansallisen sääntelyn varaan.

Keskusrikospoliisi ehdottaa, että esityksen jatkovalmistelussa arvioidaan ja selvitetään tarkemmin tarve säätää myös poliisille toimivaltuus tällaisen estomääräyksen antamiseksi rikostapauksissa. Toimivaltuus voi olla perusteltu esimerkiksi tapauksissa, joissa henkilö, jonka tietoja käytetään väärin ei kykene tai on haluton puuttumaan väärinkäytökseen tai hänen tavoittamiseen liittyy merkittävä ajallinen viive tai hän ei edes vielä tiedä, että hänen henkilötiedoillaan on esimerkiksi tehty rikoksia. Toimivaltuuden käyttö tarkoittaisi myös mahdollisuutta nopeasti estää uusien rikosvahinkojen syntymistä.

Toimivaltuus voi olla perusteltu myös siksi, että palveluntarjoajien joukko laajenee perinteisen pankkisektorin ulkopuolelle eikä palveluntarjoajalla ole pankkeja vastaavaa liiketaloudellista asiakkaiden varojen turvaamiseen liittyvää intressiä puuttua yksittäisiin käyttäjiin kohdistuviin väärinkäytöksiin. Meneillään on lakiuudistuksia, joissa pankeille ollaan säätämässä myös vahvempaa vastuuta asiakkaille aiheutuvien vahinkojen estämisessä ja korvaamisessa (PSD3 ja PSR). Nyt kyseessä olevilla palveluntarjoajille ei ilmeisesti olla säätämässä vastaavaa vastuuta.

Tunnistautumispalvelua voidaan käyttää myös EU laajuisesti. Poliisi tekee tällä hetkellä tiivistä yhteistyötä pankkien kanssa petosten torjumiseksi. Nimenomaisen poliisin toimivaltuussäännöksen puuttuessa palveluntarjoajien toiminta pohjautuisi havaituissa rikostapauksissa siten vapaaehtoisuuteen.

Eurooppalaisen digitaalisen identiteetin lompakon käyttöönotto alaikäiselle

Laki rajat ylittävästä sähköisestä tunnistamisesta, sähköisistä luottamuspalveluista ja eurooppalaisesta digitaalisesta identiteetistä 7 §

Keskusrikospoliisi kiinnitti huomiota siihen, että jo 13 -vuotias voisi lakiehdotuksen mukaan ottaa käyttöön EUDI:n itsenäisesti. Laissa 13 - vuotiaalle asetetaan korkea huolehtimisvelvoite ankaralla vastuulla ja poiketaan hallintolain 14 § omaksutusta 15-vuoden ikärajasta. Vaikka rikosoikeudellisen vastuun ikäraja on 15-vuotta vahingonkorvausvastuulla ei ole vastaavaa ikärajaa. Oletettavaa on, että 13-vuotias ei sähköisessä ympäristössäkään voi tehdä varallisuusarvoltaan merkittäviä oikeustoimia mutta huomioiden verkkoympäristön tarjoamien palveluiden laajuus, riskejä voi liittyvä siihen, että 13-vuotias ei vielä ymmärrä tai hahmota sitoumustensa kokonaisuutta ja palvelun käyttöön liittyviä vastuita, esimerkiksi toiselle henkilölle luovuttamisen osalta.

Keskusrikospoliisi ei näe syytä sille, miksi EUDI:n osalta olisi aihetta poiketa hallintolain 14 § omaksutusta ikärajaista, joka on jo kansallisesti vakiintunut.

Tunnistusvälineen itsehallinta, vaarantuminen ja tieto mihin palveluihin tunnistusvälinettä on käytetty

Laki rajat ylittävästä sähköisestä tunnistamisesta, sähköisistä luottamuspalveluista ja eurooppalaisesta digitaalisesta identiteetistä 6 §

Laki vahvasta sähköisestä tunnistamisesta 24 §

KRP katsoo, että esitutkinnallisesti sekä lisävahinkojen estämiseksi on tärkeää, että pystytään saamaan tieto mihin kaikkeen tunnistusvälinettä on käytetty sen hallinnan menettämisen jälkeen. Lisäksi olisi tärkeä rikostutkinnallisesti, että saatavilla on myös tieto siitä, millä laitteella (yksilöivä laitetieto) tunnistusväline on otettu käyttöön ja käytetty. Tämä tieto olisi tallennettava osana tarvittavia asiakasta koskevia tietoja. Keskusrikospoliisi ehdottaa laki täydennettäväksi tältä osin.

Itsehallinnan periaate vaikuttaa estävän tiedon saamisen keskitetysti muualta kuin EUDI käyttäjältä eli taholta, jonka hallussa EUDI on. Vain EUDI käyttäjä näkee kokonaiskuvan siitä, mihin palveluihin EUDI:ta on käytetty. Väärinkäytöstilanteessa EUDI voi olla rikollisen hallussa. EUDI tarjoajalla tai rikoksen uhrilla ei ole pääsyä tähän tietoon. Tähän ratkaisuun on päädytty yksityisyyden suojaamiseksi.

Väärinkäytöstilanteissa tämä on erittäin ongelmallinen tilanne. Rikostutkinnassa tavanomainen tilanne on se, että rikoksen tekijä on voinut tehdä lainahakemuksia, osamaksusopimuksella tilauksia ja muita sitoumuksia, jotka ilmenevät vasta, kun laskut alkavat saapua tai käydä lataamassa asianomistajan tietoja vaikkapa OmaKanta-palvelusta. Keskusrikospoliisi ehdottaa arvioitavaksi tuleeko ehdotettua kansallista sääntelyä uudelleenarvioida tältä osin eIDAS asetuksen antamissa rajoissa rikoksen uhrin ja viranomaisten tiedonsaantioikeuden turvaamiseksi.

Tunnistuspalveluiden ketjuttaminen ja EUDI pohjautuvien muiden tunnistusvälineiden peruminen, ensitunnistamisen kieltäminen

Laki vahvasta sähköisestä tunnistamisesta 18 a §

Tunnistuspalveluiden ketjuttaminen on merkittävä haaste rikostorjunnallisesti. Jo tällä hetkellä rikostutkinnassa on runsaasti havaintoja tapauksista, joissa rikolliset ovat saaneet haltuunsa pankkitunnukset ja niillä on hankittu mobiilivarmenne. Mobiilivarmenne taas mahdollisti jonkin aikaa toisen mobiilivarmenteen luomisen. Tämä mobiilivarmenne-mobiilivarmenne -ketjutus on nyt estetty joidenkin palveluntarjoajien toimesta rikosten estämiseksi mutta toimenpide on pohjautunut palveluntarjoajien harkintaan ja riskein hallintaan pohjautuvaan arvioon ja viranomaisten aloitteellisuuteen asiassa. Kun mobiilivarmenne otettiin aikanaan käyttöön, tuli asiakkaan käydä fyysisesti tunnistautumassa palveluntarjoajan toimipisteellä sen aktivoimiseksi. Tästä palveluntarjoajat luopuivat ja nykyään mobiilivarmenteen saa operaattorin verkkosivuilta pankkitunnuksilla tunnistautumalla.

Tilanne on haastava myös siksi, että EUDI käytön estolla tai varmenteen peruttamisella ei nyt ehdotetussa mallissa voida estää uusien luotujen tunnistusvälineiden käyttöä. Peruminen ei ilmeisesti teknisesti ”ulotu” uusiin luotuihin tunnisteisiin. Edellisessä kappaleessa kuvatulla tavalla niistä ei välttämättä edes saada selvitystä, ellei rikosentekijän päätelaitetta, jolla EUDI:ta käytetään, saada poliisin haltuun. Vain poliisilla olisi toimivaltuus ylipäänsä selvittää näitä tilanteita.

Ensimmäisen tunnistamisen kielto tulisi, sen sijaan että käyttäjän on mahdollista sitä pyytää, asettaa oletusarvoiseksi tunnistuspalvelun palveluntarjoajalla. Käyttäjän tulisi erikseen sallia ensimmäisen tunnistamisen nimenomaisesti ja ymmärtää siihen liittyvät riskit ja vaikutukset. Keskusrikospoliisi ehdottaa, että eIDAS asetuksen antamissa rajoissa arvioidaan, onko tällainen sääntely kansallisessa laissa mahdollinen. Jos tunnistusväline on jo lähtökohtaisesti väärissä käsissä ja rikollisen hallinnassa tälläkään kiellolla ei voida vaikuttaa tunnistusvälineiden ketjutusongelmaan.

Viranomaisten toimivaltuudet puuttua palveluntarjoajien toimintaan

Laki rajat ylittävistä sähköisistä tunnistamisesta, sähköisistä luottamuspalveluista ja

eurooppalaisesta digitaalisesta identiteetistä 31 - 32 §

Lain noudattamista valvoo toimijoiden osalta Liikenne- ja viestintävirasto. Lakiehdotuksen 31 - 32 §:n mukaan Liikenne- ja viestintävirastolla on oikeus tehdä toimijaa ja sen tarjoamaa palvelua koskeva tarkastus ja määrätä toimijan keskeyttämään tai lopettamaan palvelun tarjoamisen tai hyväksytyjen luottamuspalvelujen osalta peruuttaa palvelun tarjoajan tai sen tarjoaman palvelun hyväksytyin aseman.

Päätöstä tehtäessä Liikenne- ja viestintäviraston tulee ottaa huomioon velvoitteiden noudattamiseen liittyvän puutteen laajuus, kesto ja seuraukset. Yksityiskohtaisten perustelujen mukaan (s. 68) määräys palvelun tarjoamisen keskeyttämisestä tai lopettamisesta tai hyväksytyin

aseman peruuttamisesta tulisi kyseeseen vain merkitykseltään huomattavissa ja pitkäkestoisissa säännösten asettamien velvoitteiden noudattamisen puutteissa.

Keskusrikospoliisi huomauttaa, että peruuttamiskynnystä ei tule asettaa liian korkeaksi (vain merkitykseltään huomattavissa ja pitkäkestoisissa). Haavoittuvuustilanteessa palveluntarjoajan toimintaan pitäisi pystyä reagoimaan nopeasti, ellei palveluntarjoaja kykene varmistamaan palvelunsa turvallisuutta. Haavoittuvuutta hyödyntämällä rikolliset voivat aiheuttaa nopeasti ja laajasti merkittävää vahinkoa paitsi palvelun käyttäjille mutta myös koko luottamusjärjestelmälle.

Huomiot koskien digitaalista henkilöllisyystodistusta:

-

Huomiot kansallisen vahvan sähköisen tunnistamisen turvallisuutta parantavista muutoksista:

-

Huomiot koskien kansallista ekosysteemikuvausta:

-

Jaakkola Anu
Keskusrikospoliisi