Vastaus kirjalliseen kysymykseen KKV 802/2020 vp

Vastaus kirjalliseen kysymykseen Psykoterapiakeskus Vastaamon tietovuodon esiin tuomista ongelmista

Eduskunnan puhemiehelle

Eduskunnan työjärjestyksen 27 §:ssä mainitussa tarkoituksessa Te, Arvoisa puhemies, olette toimittanut asianomaisen ministerin vastattavaksi kansanedustaja Eeva-Johanna Elorannan /sd näin kuuluvan kirjallisen kysymyksen KK 802/2020 vp:

> *Mihin toimenpiteisiin hallitus aikoo ryhtyä potilasrekisterien tietoturvan varmistamiseksi ja valvomiseksi, identiteettivarkauden uhrien suojaamiseksi sekä tietoturvalainsäädännön ajantasaistamiseksi mm. henkilötunnuksen sijasta vahvan tunnistautumisen velvoittamiseksi mm. kaupassa, verkkokaupassa ja viranomaisasioinnissa sekä perintätoimessa?*

Vastauksena kysymykseen esitän seuraavaa:

Tietoturvallisuuden lainsäädäntöä on kehitetty viime vuosina ja kehitetään edelleen vastamaan entistä paremmin digitaalisen yhteiskunnan vaatimuksiin. Tietoturvaan liittyvää sääntelyä on useissa eri laeissa ja viimeisimpänä tuli voimaan laki julkisen hallinnon tiedonhallinnasta (906/2019), jonka 4. luvussa säädetään julkisen hallinnon tietojärjestelmiin liittyvistä yleisistä tietoturvallisuusvelvollisuuksista. Oikeusministeriön vastuulle kuuluva yleinen tietosuojalainsäädäntö on uudistunut vuonna 2018, kun EU:n yleistä tietosuoja-asetusta (2016/679) alettiin soveltaa. Yleistä tietosuojasääntelyä voi pitää varsin ajantasaisena. Yleinen tietosuojalainsäädäntö edellyttää, että henkilötietoja käsitellään lainmukaisesti ja tietoturvallisesti. Tietojärjestelmät on suunniteltava tavalla, jossa huomioidaan tietosuoja oletusarvoisesti. Kun käsittelyyn liittyy riskejä esimerkiksi siksi, että käsitellään hyvin arkaluonteisia tietoja, on tiedot turvattava erityisen huolellisesti. Rekisterinpitäjä vastaa ja sen on pystyttävä osoittamaan, että se on noudattanut henkilötietojen käsittelyä koskevia periaatteita. Henkilötietojen tietoturvaloukkauksesta on tietosuojalainsäädännön mukaan myös ilmoitettava tietosuojavaltuutetulle ja tietyissä tilanteissa myös loukkauksen uhreille.

Potilasrekistereiden tietoturvaa koskevasta sääntelystä vastaa sosiaali- ja terveysministeriö. Sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevassa laissa (159/2007, asiakastieto-laki) säädetään mm. sosiaali- ja terveydenhuollon palvelunantajien tietoturvaa ja tietosuojaa koskevasta oma-valvontasuunnitelmasta, palvelunantajien ja tietojärjestelmän valmistajien vastuista, asiakas- ja potilastietoja käsittelevien tietojärjestelmien tietoturvavaatimuksista sekä valvonnasta. Asiakastietolaissa säädetään myös tietojärjestelmien kuulumisesta A-ja B-luokkiin. A-luokkaa ovat kaikki Kanta-palveluun liitettävät asiakas- ja potilastietojärjestelmät, B-luokkaa ne järjestelmät, joita ei ole tarkoitettu liitettäväksi Kanta-palveluun.

Vastaus kirjalliseen kysymykseen KKV 802/2020 vp

Kanta-palveluihin liitettävät tietojärjestelmät on sertifioitava ennen liittymistä Kanta-palveluun. Monet asiakastietolain mukaisista vaatimuksista koskevat kuitenkin kaikkia asiakas- ja potilastietojärjestelmiä. Esimerkiksi tietojärjestelmiä koskevat olennaiset vaatimukset, tietojärjestelmän valmistajan yleiset velvollisuudet sekä valvonta koskevat yhtä lailla niin A- kuin B-luokan järjestelmiä. Myös palvelunantajan vastuu omavalvontasuunnitelmasta koskee myös Kantaan liittymättömiä palvelunantajia, samoin palvelunantajan vastuu ilmoittaa tietojärjestelmän poikkeamista sosiaali- ja terveysalan lupa- ja valvontavirasto Valviralle. Palvelun-antajan on myös seurattava ja valvottava, että sen antamaan palveluun liittyvä tietosuoja ja tietoturva toteutuvat.

Valvonnan osalta asiakastietolaissa säädetään palvelunantajan valvontavastuusta. Valviran valvontavastuu koskee sekä A- että B-luokan järjestelmiä, ja molempiin luokkiin kuuluvat järjestelmät on ilmoitettava Valviran tietojärjestelmärekisteriin. Samoin valvonnan keinot ovat samat kaikille tietojärjestelmille, esim. määräys tuotantokäytössä olevan järjestelmän puutteiden korjaamisesta, tietojärjestelmän käytön kieltäminen ja uhkasakko. Valvontaviranomaisen toteuttaman valvonnan laajuudesta riippumatta keskeistä on kuitenkin edelleen kunkin palvelunantajan vastuu tietoturvan toteutumisesta omassa toiminnassaan ja järjestelmissään.

Hallitus on antanut eduskunnalle asiakastietolakia koskevan muutosesityksen (HE 212/2020 vp). Siinä esitetään liittymisvelvoitetta Kanta-palveluihin kaikille sosiaali- ja terveydenhuollon toimijoille, joilla on käytössään potilas- tai asiakastietojärjestelmä. Tämä tarkoittaa sitä, että suuri joukko nyt sertifioinnin ulkopuolelle jääneitä B-luokan järjestelmiä siirtyy A-luokkaan ja niille on tehtävä ulkopuolisen tahon suorittama sertifiointi.

Henkilötunnuksen käyttötapoihin vaikuttaa myös se, missä määrin voimassaolevassa lainsäädännössä on asetettu vaatimuksia henkilöllisyyden todentamiseksi erilaisissa asiointitilanteissa. Viranomaisasiointi pohjautuu hallintolakiin. Hallintolain 16 §:n mukaan viranomaiselle toimitettavasta asiakirjasta on käytävä ilmi, mitä asia koskee. Asiakirjassa on mainittava lähettäjän nimi sekä tarvittavat yhteystiedot asian hoitamiseksi. Hallintolain 19 §:n mukaan asia pannaan vireille kirjallisesti ilmoittamalla vaatimukset perusteineen. Viranomaisen suostumuksella asian saa panna vireille myös suullisesti. Tämä sääntely merkitsee sitä, ettei vireillepanon yhteydessä henkilöä tarvitse tunnistaa eikä esimerkiksi paperiasioinnissa vaadita passikopiota tai muuta henkilöllisyyden osoittavan asiakirjan kopiota hakemuksen liitteeksi, vaan riittää kun hakijan voidaan yksilöidä riittävän luotettavasti hakemuksen perusteella. Vastaava toimintamalli on mahdollista myös digitaalisessa toimintaympäristössä, jossa esimerkiksi sähköpostilla toimitettu vapaamuotoinen hakemus viranomaisen tulee käsitellä, jos sitä käy ilmi mitä asiaa hakemus koskee. Asioitaessa viranomaisten digitaalisten palvelujen avulla vahvaa sähköistä tunnistamista on käytettävä, jos digitaalisesta palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi.

Vahvaa sähköistä tunnistamista vaaditaan pääsääntöisesti jo nykyisin kuluttajansuojalain (38/1978) mukaan, kun kuluttaja tekee kuluttajaluottosopimuksen luotonantajan kanssa sähköisesti eikä häntä ole aikaisemmin tunnistettu laissa edellytetyllä tavalla. Lakiin sisältyy kuitenkin eräitä poikkeuksia. Vaatimus vahvasta sähköisestä tunnistamisesta ei koske hyödykesidonnaisia kertaluottoja, joita tyypillisesti tarjotaan yhtenä rahoitusvaihtoehtona verkkokaupassa. Lisäksi

Vastaus kirjalliseen kysymykseen KKV 802/2020 vp

maksupalvelulaissa (290/2010) on vahvan tunnistamisen käyttöä edellyttävää sääntelyä, joka soveltuu esimerkiksi tilanteissa, joissa henkilö ostaa verkkokaupasta hyödykkeen ja maksaa sen verkkopankkinsa kautta taikka maksukortilla tai muulla maksuvälineellä.

Oikeusministeriössä tullaan keväällä 2021 käynnistettävän kuluttajaluottosäännösten uudistamista koskevan hankkeen yhteydessä arvioimaan, tuleeko henkilöllisyyden todentamisvelvollisuutta koskevaa sääntelyä tiukentaa laajentamalla se koskemaan kaikkien kuluttajaluottosopimusten tekemistä. Kun henkilöllisyyden todentamista koskevat säännökset lisättiin kuluttajansuojalakiin vuonna 2009, tiedossa olivat lähinnä ns. pikaluottoihin liittyvät ongelmat.

Saatavien perinnästä annetussa laissa (513/1999) edellytetään, että perinnässä noudatetaan hyvää perintätapaa. Hyvään perintätapaan kuuluu, ettei lainvastaisia tai selvästi perusteettomia saatavia oteta perittäviksi (HE 199/1996, s. 11-12). Perintätoimeksiannon saajalla ei kuitenkaan hyvän perintätavan nojalla ole katsottava olevan yleistä velvollisuutta ryhtyä selvittämään saatavan oikeellisuutta, ml. sitä, onko sen sopimuksen tekemisessä, johon perittävä saatava perustuu, käytetty vahvaa sähköistä tunnistamismenetelmää. Huomioon ottaen toiminnan massaluonteisuus ei voida myöskään pitää tarkoituksenmukaisena tällaista velvollisuutta perintätoimeksiannon saajille asettaa.

Velallisen suojaksi perintälaissa myös säädetään, että saatavan vapaaehtoista perintää ei saa jatkaa, jos velallinen kiistää maksuvelvollisuutensa. Perintää saa kiistämisestä huolimatta jatkaa, jos velallinen ei esitä kiistämiselle perustetta tai vetoaa ainoastaan sellaiseen perusteeseen, jolla selvästi ei ole vaikutusta velallisen maksuvelvollisuuteen. Mikäli velallinen esim. perintäkirjeen saatuaan ilmoittaa, ettei hän ole kyseistä saatavan perusteena olevaa oikeustoimea tehnyt, ei vapaaehtoista perintää voisi lähtökohtaisesti jatkaa ainakaan ennen asian tarkempaa selvittelyä.

Yksi suojakeino väärinkäytöksien torjumiseen on luottotietorekisteriin tehtävä vapaaehtoinen luottokieltomerkintä. Tilanne on tällä hetkellä se, että luottotietotoimintaa harjoittavat ainoastaan yksityiset elinkeinonharjoittajat. Luotonmyöntöä harkitessaan luotonantajat säännönmukaisesti tarkastavat luotonhakijan luottotiedot näistä yksityisten toimijoiden ylläpitämistä rekistereistä. Tällä hetkellä ei ole käytössä sellaista viranomaisrekisteriä, johon tieto vapaaehtoisesta luottokiellosta voitaisiin mielekkäästi tallettaa.

Parhaillaan oikeusministeriössä kuitenkin valmistellaan uutta positiivista luottotietorekisteriä, joka tulisi olemaan viranomaisen ylläpitämä. Osana positiivisen luottotietorekisterin valmistelua pyritään toteuttamaan rekisteriin vapaaehtoisen luottokiellon mahdollisuus. Tällöin vapaaehtoisen luottokiellon tekeminen voisi vastaisuudessa olla maksutonta.

Psykoterapiakeskus Vastaamoon kohdistuneen tietomurron ja mahdollisten vastaavanlaisten tapausten seurausten lieventämiseksi on ehdotettu perustettavaksi keskitettyä viranomaisen ylläpitämää sähköistä palvelua helpottamaan ja yksinkertaistamaan tietomurron uhrien toimintamahdollisuuksia. Digi- ja väestötietoviraston Suomi.fi - palveluun on jo nyt koottu oleelliset asiaan liittyvät tiedot, ohjeet ja linkit, niin että identiteettivarkauden uhri voi mahdollisimman helposti ja mahdollisimman vähillä toimenpiteillä saada voimaan tarvitsemansa estot ja kiellot. Lisäksi

Vastaus kirjalliseen kysymykseen KKV 802/2020 vp

valtiovarainministeriö käynnistää lainsäädäntöselvityksen keinoista rakentaa julkisen ja yksityisen sektorin yhteinen keskitetty estojen ja kieltojen asettamisen palvelu osaksi Suomi.fi – palvelua. Tavoitteena on, että henkilö joka on joutunut identiteettivarkauden uhriksi tai on uhka, että on joutumassa, pystyisi kirjautumaan yhteen viranomaisjärjestelmään, mistä voisi hakea erilaiset kiellot ja estot yhdestä paikasta.

Keskitetyn sulkupalvelun lisäksi hallitus valmistelee sekä lyhyen että pidemmän aikavälin toimenpiteitä henkilötunnuksen käyttöön ja muuttamiseen liittyen. Lyhyen aikavälin toimenpiteiden tavoitteina on edistää henkilötunnuksen käyttötapoja yhteiskunnassa. Toimenpiteiden tavoitteena on vähentää henkilötunnuksella tehtävien väärinkäytösten mahdollisuuksia ja vähentää tietoturvaloukkausten ja tieto- ja viestintärikosten uhreiksi joutuneille aiheutuvaa vahinkoa vääriin käsiin joutuneista identiteettitiedoista. Hallitus aloittaa valmistelemaan lakimuutosta, joka rajatuissa tilanteissa, kuten tietomurtojen yhteydessä, antaa mahdollisuuden muuttaa henkilötunnusta identiteetin väärinkäyttämisen rajoittamiseksi. Lisäksi henkilötunnuksen käyttöä koskevia edistämistoimia, kuten kansalaisten informoimista ja hyvien käytäntöjen ohjaamista voidaan toteuttaa lyhyellä aikavälillä tämän vuoden loppuun mennessä asetettavassa henkilötunnuksen uudistamishankkeessa.

Helsingissä 17.11.2020

Kuntaministeri Sirpa Paatero