23.11.2020

Julkisen hallinnon tieto- ja viestintätekninen osasto

Arviomuistio henkilötunnuksen muuttamista koskevan lainsäädännön uudistamisesta

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto

puh. 0295 16001 (vaihde)
valtiovarainministerio@vm.fi
www.vm.fi
Y-tunnus 0245439-9

Finansministeriet
Snellmansgatan 1 A, Helsingfors
PB 28, 00023 Statsrådet

tfn 0295 16001 (växel)
valtiovarainministerio@vm.fi
www.finansministeriet.fi
FO-nummer 0245439-9

Sisällysluettelo

Tiivistelmä 3
1. Johdanto 4
2. Nykytila ja sen arviointi 4
2.1. Henkilötunnuksen tarkoitus 4
2.2. Henkilötunnuksen muuttamista koskeva sääntely 5
2.3. Henkilötunnuksen nykyisiin käsittelytapoihin liittyviä ongelmia 7
2.4. Henkilötunnuksen muuttamisen hyödyt ja haitat 9
2.5. Tieto- ja viestintärikoksia koskeva sääntely 10
2.6. Sääntelyn arviointi 10
3. Sääntelyvaihtoehdot 11
3.1. Yleisesti sääntelyvaihtoehdoista 11
3.2. Vaihtoehto 1: Kaksivaiheinen menettely tietoturvaloukkauksen johdosta 12
3.3. Vaihtoehto 2: Yksivaiheinen menettely tietomurron johdosta 14
3.4. Perustuslaillisista näkökohdista 17
3.4.1. Henkilötunnus turvaa henkilön oikeuksia ja velvollisuuksia 17
3.4.2. Yhdenvertaisuus 17
4. Vaikutukset 19
4.1. Vaikutukset identiteettivarkauksien ja muiden rikollisissa tarkoituksessa tehtävien tekojen ehkäisyyn 19
4.2. Vaikutukset kansalaisille, henkilötunnusta hyödyntäville tahoille ja Digi- ja väestötietovirastolle 20
4.3. Vaikutukset henkilötunnusjärjestelmään 21
5. Muut toteuttamisvaihtoehdot ja kehityshankkeet 22
5.1. Lyhyen aikavälin toimenpiteet 23
5.1.1. Henkilötunnuksen käsittelyä koskevien käytäntöjen ohjaus 23
5.1.2. Henkilötietojen sulku- ja estopalvelujen kokoaminen 24
5.2. Pidemmän aikavälin toimenpiteet 24
5.2.1. Digitaalinen henkilöllisyys ja tunnistaminen 24
5.2.2. Digitaalinen turvallisuuden periaatepäätöksen toimeenpano 25
5.2.3. Henkilöllisyyden todentamisen toimintamallien ja lainsäädännön kehittämistarpeiden selvittäminen 25
5.2.4. Kuluttajasuojalaki 26

Tiivistelmä

Tämän muistion tarkoituksena on arvioida sääntelymuutostarpeita, jotka liittyvät henkilötunnuksen muuttamisen edellytyksiin. Sääntelymuutoksella pyritään turvamaan sellaisten henkilöiden oikeudet, joiden henkilötiedot ovat joutuneet tietomurron tai tietoturvaloukkausten kohteeksi. Tämä kysymys on tarkastelussa erityisesti Psykiatrikeskus Vastaamon tietomurtotapaukseen liittyen ja sen ilmentämänä yhteiskunnallisena tarpeena.

Henkilötunnus on tarkoitettu henkilöiden yksilöimiseen, eikä henkilötunnuksen perusteella ketään henkilöä voida tunnistaa tai henkilöllisyyttä varmistaa luotettavasti. Henkilötunnusjärjestelmän perustana on se, että henkilötunnus on ainutkertainen, pysyvä ja muuttumaton. Kolmannen osapuolen haltuun joutuneella henkilötunnuksella voidaan aiheuttaa jossain määrin vahinkoja tai oikeudenloukkauksia asianosaiselle. Yksilön suojaamisen ja aseman kannalta henkilötunnuksen muuttamisella identiteettivarkaustilanteessa tai muissa henkilöllisyyteen liittyvissä rikoksissa on sekä hyötyjä että haittoja. Henkilötunnuksen muuttaminen ei aukottomasti poista petosten tekomahdollisuutta varastetulla identiteetillä.

Henkilötunnuksen muuttamisesta säädetään väestötietojärjestelmästä ja Digi- ja väestötietojärjestelmän varmennepalveluista annetun lain (661/2009), jatkossa *VTJ-laki*, 12 §:ssä. Kyseessä on tyhjentävä ja hyvin suppeasti sovellettava säännös, jolla poiketaan henkilötunnuksen pysyvyyden ja muuttumattomuuden lähtökohdista. Säännöksen perusteella henkilötunnuksen muuttamista koskevat edellytykset ovat sovellettavissa henkilötunnuksen väärinkäyttötilanteessa vain, kun yksilölle on jo aiheutunut väärinkäytöksistä merkittävää haittaa. Henkilötunnus ja sen käsittely ovat merkityksellisiä perustuslaissa turvattujen perusoikeuksien toteuttamiselle sekä yhdenvertaisuuden osalta.

Henkilötunnuksen muuttamista koskevan sääntelymuutoksen valmistelussa on otettava huomioon esimerkiksi henkilötunnuksen pysyvä luonne, viranomaisten mahdollisuudet ja toimivalta arvioida tapahtuneen loukkauksen lainvastaisuutta sekä käytännön vaikutukset henkilötunnuksen muuttamisesta. Keskeistä on, että tunnuksen muuttamisen tulisi aina tapahtua henkilön omasta hakemuksesta. Muistiossa kuvataan kaksi sääntelyvaihtoehtoa VTJ-lain 12 §:n muuttamiseksi.

Muistiossa on arvioitu henkilötunnuksen muuttamisen kriteeristön muuttamisen vaikutuksia esimerkiksi identiteettivarkauksien ehkäisyyn, kansalaisiin sekä Digi- ja väestötietovirastoon.

Lisäksi arvioidaan muita toimia, joilla edistettäisiin henkilötunnuksen asianmukaisia käsittelytapoja ja vahvistettaisiin yleisesti luotettavien ja tietoturvallisten menettelyjen käyttöä asioitaessa yhteiskunnan eri palveluissa ja toiminnoissa. Lyhyen aikavälin tunnistettuja toimenpiteitä ovat henkilötunnuksen käsittelyä koskevan käytännön ohjaus sekä henkilötietojen sulku- ja estopalveluiden yhteenkokoaminen. Pidemmän aikavälin toimenpiteitä ovat esimerkiksi Digitaalisen henkilöllisyyden hankkeen jatkaminen sekä digitaalisen turvallisuuden periaatepäätöksen toimeenpano.

1. Johdanto

Tarve arvioida henkilötunnuksen muuttamista koskevaa sääntelyä on noussut esille Psykiatriakeskus Vastaamon tietomurron yhteydessä. Tapaus on poliisin esitutkinnassa. Kyse on erittäin laajasta tietomurrosta, joka koskee isoa määrää ihmisiä. Tietomurron johdosta tapahtuneessa tietovuodossa on vuotanut myös henkilöiden arkaluonteisia asiakastietoja. Tiedot ovat mahdollisesti levinneet internetissä laajasti kolmansien osapuolien käsiin. Tietoja on käytetty muun muassa kiristystarkoituksissa.

Käsillä oleva tapaus on yksittäinen, vaikkakin merkittävä ja laajavaikutteinen. Se tuo kuitenkin esiin yhteiskunnan muutosta entistä verkottuneemmaksi myös rikollisten toimien näkökulmasta. Tilastokeskus tekee tilastoja ilmoitetuista rikoksista. Viranomaisten tietoon tulleita tietomurtorikoksia on viimeisen vuosikymmenen aikana ollut vuosittain joitakin satoja. Lukumäärä on vaihdellut vuosittain noin 300 ja 800 välillä. Vuonna 2019 määrä on ollut suurin. Selkeää trendiä tietomurtorikosten kasvusta ei tilastojen perusteella kuitenkaan ole pääteltävissä. Vuonna 2017 on ollut merkittävä piikki törkeissä tietomurtorikoksissa. Identiteettivarkaus on säädetty rikoslakiin (39/1889) vuonna 2015. Sen jälkeen niitä on tilastoitu viranomaisten tietoon tulleiksi 3000 – 4000 vuosittain.

Edellä mainitut tilastot eivät kerro sitä, kuinka paljon rikollisesti hankittuja tai erilaisten tietovuotojen vuoksi kolmansien haltuun joutuneita henkilötietoja on käytetty muussa rikollisessa toiminnassa kuten petoksenteon välineenä tai kiristystarkoituksissa. Voidaan arvioida, että kiristystarkoitus on jossain määrin uusi ilmiö.

Käsillä oleva rikos on tuonut esiin tarpeen arvioida sääntelymuutostarpeita yhteiskuntakehityksestä johtuvista syistä. Yksilön oikeuksien loukkauksia on entistä laajemmin mahdollista tehdä sähköisien asiointipalvelujen avulla ja internetissä yleisesti. Tällainen kehitys on mahdollistanut myös entistä laajempia ja yleisesti vahingollisempia tieto- ja viestintärikoksia, kuten tietomurtoja. Myös tietoturvaloukkaukset, jotka eivät täytä tietomurron tunnusmerkistöjä, voivat johtaa laajoihin ja pitkäaikaisiin henkilötietojen väärinkäytöksiin.

Muistiossa arvioidaan voimassa olevaa henkilötunnuksen muuttamisen kannalta keskeistä sääntelyä ja siihen liittyviä sääntelymuutostarpeita, eri sääntelyvaihtoehtoja sekä muita henkilötunnuksen asianmukaisia käsittelytapoja edistäviä toimenpiteitä yhteiskunnassa. Lisäksi muistiossa arvioidaan henkilötunnusta koskevan sääntelyn muuttamisesta seuraavia vaikutuksia.

2. Nykytila ja sen arviointi

2.1. Henkilötunnuksen tarkoitus

Väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (VTJ-laki 661/2009) 11 §:n mukaan, kun henkilön tiedot talletetaan ensimmäisen kerran väestötietojärjestelmään, hänelle on annettava henkilötunnus. Henkilötunnus annetaan automaattisesti väestötietojärjestelmästä. Korjattua tai muutettua henkilötunnusta ei saa antaa toiselle henkilölle.

Henkilötunnuksen tallentamisella väestötietojärjestelmään luodaan edellytykset jokaiselle toimia suomalaisessa yhteiskunnassa oikeuksiensa ja velvollisuuksiensa toteuttamiseksi. Henkilötunnuksen ja muiden keskeisten tietojen rekisteröimisellä valtion ylläpitämään rekisteriin muodostetaan jokaiselle yksilöllinen rekisteröity henkilöllisyys, jota voidaan hyödyntää laajasti yhteiskunnan toiminnoissa.

Henkilötunnus on tarkoitettu henkilöiden yksilöimiseen eli erottamaan henkilö muista, esimerkiksi samannimisistä, henkilöistä. Lähtökohtaisesti henkilötunnus ja sen käsittelymenettelyt ovat toimineet ja toimivat hyvin siinä tarkoituksessa johon se on tarkoitettu. Henkilötunnuksen avulla voidaan yksilöidä henkilöitä tietojärjestelmissä sekä esimerkiksi laskujen perinnässä, palkanmaksussa ja terveydenhuollossa. Nykyinen henkilötunnusjärjestelmä mahdollistaa myös eri palvelutuottajien tarjoamien palvelujen ja niissä olevien yhdistämisen samaan henkilöön.

Tietosuojavaltuutettu on useassa yhteydessä korostanut, että henkilötunnusta ei ole tarkoitettu henkilöiden tunnistamiseen, vaan yksilöimiseen. Henkilötunnus voi olla myös muiden kuin asianomaisen tiedossa, mikä myös mahdollistaa tunnuksen väärinkäytön esimerkiksi niissä tilanteissa, joissa käytännöksi on muodostunut käyttää henkilötunnusta asiakkaan tunnistamisen keinona.

Henkilötunnuksen käyttötarkoituksista ja käsittelyn edellytyksistä säädetään kansallisessa tietosuojalaissa (1050/2018). Sen 29.1 §:n mukaan henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää: 1) laissa säädetyn tehtävän suorittamiseksi; 2) rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi; tai 3) historiallista tai tieteellistä tutkimusta taikka tilastointia varten. Edelleen mainitun lain 29.2 §:n mukaan henkilötunnusta saa käsitellä luotonannossa tai saatavan perimisessä, vakuutus-, luottolaitos-, maksupalvelu-, vuokraus- ja lainaustoiminnassa, luottotietotoiminnassa, terveydenhuollossa, sosiaalihuollossa ja muun sosiaaliturvan toteuttamisessa tai virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa. Lisäksi lain 3 momentin mukaan henkilötunnuksen saa luovuttaa osoitetietojen päivittämiseksi tai moninkertaisten postilähetysten välttämiseksi suoritettavaa tietojenkäsittelyä varten, jos henkilötunnus jo on luovutuksensaajan käytettävissä.

Henkilötunnus ei luo henkilölle mitään oikeuksia tai velvollisuuksia. Henkilötunnuksen ilmoittaminen tai esittäminen ei ole tae siitä, että kyseessä on henkilötunnuksen tarkoittama henkilö. Siten henkilötunnuksen perusteella ketään henkilöä ei voida tunnistaa tai henkilöllisyyttä varmistaa luotettavasti, vaan siihen tarvitaan myös muita tietoja tai henkilötodistus.

Henkilötunnuksen käyttöä tunnistamisen keinona voidaan arvioida yleisen tietosuoja-asetuksen (EU) 2016/679 velvoitteiden kannalta myös siitä näkökulmasta, että rekisterinpitäjän ja henkilötietojen käsittelijän on varmistuttava tietojen täsmällisyydestä ja oikeellisuudesta. Mikäli tunnistaminen tehdään huolimattomasti varmistumatta sen henkilön henkilöllisyydestä, jonka tietoja rekisterinpitäjä ryhtyy käsittelemään, voi rekisterinpitäjä toimia tietosuoja-asetuksen vastaisesti.

2.2. Henkilötunnuksen muuttamista koskeva sääntely

VTJ-lain 12 §:ssä säädetään henkilötunnuksen korjaamisesta ja muuttamisesta poikkeuksellisissa tilanteissa. Lain 12 §:n säännös henkilötunnuksen muuttamisesta on kriteereiltään tiukka ja suppeasti tulkittava, koska henkilötunnus on tarkoitettu muuttumattomaksi

ja pysyväksi. Säännös on muuttamisen perusteiden osalta tyhjentävä. Voimassa olevasta säännöksestä on tässä muistiossa kuvatun tavoitteen kannalta tarkasteltava erityisesti pykälän 2 momentin 1 ja 2 kohtia:

> ---
>
> *Väestötietojärjestelmään talletettu henkilötunnus voidaan muuttaa, jos:*
>
> *1) muuttaminen on ehdottoman välttämätöntä henkilön suojelemiseksi sellaisissa tilanteissa, joissa hänen terveyteensä tai turvallisuuteensa kohdistuu ilmeinen ja pysyvä uhka;*
>
> *2) muu kuin henkilötunnuksen haltija on toistuvasti väärinkäyttänyt tunnusta ja käytöstä on aiheutunut merkittävää taloudellista tai muuta haittaa tunnuksen oikealle haltijalle ja henkilötunnuksen muuttamisella voidaan tosiasiallisesti estää väärinkäytön haitallisten seurausten jatkuminen;*
>
> ---

Henkilötunnuksen muuttamisesta päättää 2 momentin 1 ja 2 kohdassa tarkoitetussa tapauksessa Digi- ja väestötietovirasto. Asianosaisen on haettava henkilötunnuksen muuttamista kirjallisesti.

Käytännössä henkilötunnuksien muuttamisia on ollut vain yksittäisiä vuosittain. VTJ-lain hallituksen esityksessä (HE 89/2008) henkilötunnuksen muuttamista koskevan säännöksen yksityiskohtaisissa perusteluissa säännöksen suppeasta tulkinnasta on todettu seuraavaa:

Keskeisin periaate ja lähtökohta momentin säännöksiä sovellettaessa olisi, että kerran annettu henkilötunnus on tarkoitettu muuttumattomaksi ja pysyväksi. Merkittävää säännöksen soveltamisalan kannalta olisi myös se, että tunnuksen muuttamisen edellytykset on säännöksessä lueteltu tyhjentävästi. Nämä lähtökohdat huomioon ottaen säännöksen tulkinta-ala olisi hyvin suppea ja se olisi tarkoitettu sovellettavaksi vain erityisen poikkeuksellisissa tapauksissa ja silloinkin vain, jos muuttamisen perusteet olisivat aivan ilmeisesti käsillä. Momentin 1 ja 2 kohdissa tarkoitetuissa tapauksissa olisi lisäksi otettava huomioon, että tunnuksen muuttaminen olisi lähtökohtaisesti poikkeuksellinen turvaamistoimi. Sen toteuttamiselle näissä tapauksissa asetetut edellytykset olisivat objektiivisia edellytyksiä eikä sitä tulisi tehdä pelkästään henkilön subjektiivisten tuntemusten perusteella.

Hallituksen esityksen perusteluissa todetaan lisäksi: *Ehdotetussa säännöksessä on menettelyä koskevan yksityiskohtaisen sääntelyn tarkoituksena ollut korostaa sitä, että tunnuksen muuttaminen on poikkeuksellinen toimenpide, joka koskee keskeisesti asianomaisen henkilön henkilöllisyyden perusteita. Säännöksellä on lisäksi tahdottu painottaa sitä, että tunnuksen muuttamisella on henkilöllisyyden määrittelyn lisäksi lukuisia vaikutuksia myös ympäröivään yhteiskuntaan.*

Edellytykset on kirjoitettu tyhjentäviksi ja niitä tulisi lain esitöiden mukaan soveltaa vain erityisen poikkeuksellisissa tapauksissa. Lakia koskevan hallituksen esityksen yksityiskohtaisissa perusteluissa on lisäksi todettu, että henkilötunnukseen liittyvän yksilöllisyyden vaatimuksen sekä tunnistusominaisuuden johdosta korjattua tai muutettua henkilötunnusta ei saa antaa toiselle

henkilölle. Tällaista niin sanottua passiivia henkilötunnusta ei kuitenkaan poistettaisi väestötietojärjestelmästä, sillä henkilön aikaisemmalla tunnuksella saattaa olla myöhemmin merkitystä esimerkiksi henkilön tunnistamisessa ja henkilöllisyyden selvittämisessä tai hänen tekemiensä oikeustoimien vaikutuksia arvioitaessa.

Voimassa olevaa sääntelyä ei voi soveltaa ennalta ehkäisevästi identiteettivarkauden tai tietomurron uhreiksi joutuneiden mahdollisten vahinkojen tai muiden oikeuden loukkausten ehkäisemiksi. Ainoastaan terveyden tai turvallisuuden vuoksi tämä on hyvin rajoitetusti mahdollista. Tällöinkin olisi yksittäistapauksittain todettava objektiivisesti tällaisen uhan olevan olemassa. Pelkästään asianosaisen subjektiivinen käsitys terveyteen kohdistuvasta uhasta ei riitä. Uhan olisi oltava myös ilmeinen ja pysyvä luonteeltaan. Näiden kriteerien olemassaoloa tietomurron uhriksi kohdistuneiden osalta on ainakaan yleisesti ja kattavasti vaikea perustella.

Henkilötunnusjärjestelmän perustana on se, että henkilötunnus on ainutkertainen, pysyvä ja muuttumaton. Voimassa olevan lainsäädännön lähtökohtana on, että henkilötunnuksen muuttaminen olisi vain hyvin poikkeuksellisesti mahdollista. Tällä on tarkoitus varmistaa se, ettei muodostuisi kaksoisidentiteettejä ja että henkilötietojen yhdistäminen eri rekistereissä olisi mahdollisimman sujuvaa ja virheetöntä.

2.3. Henkilötunnuksen nykyisiin käsittelytapoihin liittyviä ongelmia

Yhteiskunta on kehittynyt merkittävästi digitaalisemmaksi viimeisen vuosikymmenen aikana. Tämä asettaa myös henkilötunnusjärjestelmän kehittämiselle paineita. Näitä kysymyksiä on laajasti selvitetty valtiovarainministeriön asettamassa henkilötunnuksen uudistamista selvittäneessä työryhmässä.[1]

Yhteiskunnan muutos entistä digitaalisemmaksi on synnyttänyt myös uudenlaisia riskejä henkilötietojen käsittelyyn. Yksilön oikeuksien loukkauksia on entistä laajemmin mahdollista tehdä sähköisien asiointipalvelujen avulla ja internetissä yleisesti. Tällainen kehitys on mahdollistanut myös entistä laajempia ja yleisesti vahingollisempia tieto- ja viestintärikoksia, kuten tietomurtoja. Myös tietoturvaloukkaukset, jotka eivät täytä tietomurron tunnusmerkistöjä, voivat johtaa laajoihin ja pitkäaikaisiin henkilötietojen väärinkäytöksiin. Toisaalta tietoturvaloukkaukset ja tietovuodot eivät myöskään läheskään aina johda henkilötietojen väärinkäytöksiin, vaan esimerkiksi väärään paikkaan joutunut henkilötietoja sisältävä tiedosto saadaan palautettua tai tuhottua ennen kuin tiedoilla on tehty mitään vahinkoa. Myös käsillä oleva tietomurto on tuonut esiin tämän kehityksen ja samalla vahvistanut tarvetta arvioida nykyisiä toimintatapoja henkilön tunnistamisessa asiointitilanteessa sekä henkilötunnuksen käsittelyssä ja arvioida myös nykyisen sääntelyn toimivuutta.

Tätä yhteiskunnallista kehitystä kuvaa myös se, että tieto- ja viestintärikoksia koskevaa sääntelyä uudistettiin 2015, muun muassa lisäämällä rikoslakiin uutena rikoksena identiteettivarkaus. Identiteettivarkauksia on vuosittain noin 3000-4000.

Henkilötunnuksen osalta syitä käytön laajentumiselle henkilön yksilöintitehtävästä laajemmaksi voidaan hakea henkilötunnukseen liittyvästä luottamuksesta ja käytön helppoudesta. Henkilöön liittyvät viralliset henkilötiedot ylläpidetään Digi- ja väestötietoviraston väestötietojärjestelmässä.

[1] https://vm.fi/hanke?tunnus=VM068:00/2017

Käsitys henkilötunnusta koskevan tiedon luotettavuudesta on mahdollisesti osaltaan myös johtanut siihen, että henkilötunnusta käytetään yhteiskunnassa myös muuhun kuin henkilön yksilöintiin, esimerkiksi henkilön tunnistamisen välineenä. Henkilötunnuksen saanut henkilö on olemassa, ja henkilötunnusta on pidetty helppona ja riittävän luotettavana tietona, jolla voidaan todentaa henkilön henkilöllisyys erilaisissa asiointitilanteissa. Ongelma ei siis yksistään poistu henkilötunnuksen muotoa tai yksittäisen henkilön henkilötunnusta muuttamalla, vaan muuttamalla koko henkilön identiteetinhallinnan ja -hyödyntämisen prosessit vastaamaan digitaalisen toimintaympäristön vaatimuksia.

Henkilötunnuksella ja joillain muilla henkilön yksilöivillä tiedoilla, kuten nimi ja osoite, on mahdollista toimia väärällä identiteetillä joissakin tilanteissa, koska henkilötunnuksen käyttötavoista on muodostunut sellaisia, että tunnusta käytetään tunnistamisessa. Väärää identiteettiä voidaan hyödyntää sellaisissa tilanteissa, joissa toimija mahdollistaa henkilöllisyyden todentamisen tietoturvatasoltaan heikolla tavalla.

Henkilötunnuksen käyttötapoihin vaikuttaa myös se, missä määrin voimassa olevassa lainsäädännössä on asetettu vaatimuksia henkilöllisyyden todentamiseksi erilaisissa asiointitilanteissa.

Viranomaisasiointi pohjautuu vahvasti hallintolakiin (434/2003). 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 hakemuksen liitteeksi, vaan riittää kun hakijan voidaan yksilöidä riittävän luotettavasti. Vastaava toimintamalli on luonnollisesti mahdollista myös digitaalisessa toimintaympäristössä, jossa esimerkiksi sähköpostilla toimitettu vapaamuotoinen hakemus tulee käsitellä, jos sitä käy ilmi mitä asiaa hakemus koskee. Asioitaessa viranomaisten digitaalisten palvelujen avulla vahvaa sähköistä tunnistamista on käytettävä digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) 6.2 §:n perusteella, jos digitaalisesta palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi.

Laissa on myös mahdollista säätää henkilöllisyyden todentamista koskevista velvoitteista sopimusta tehtäessä, kuten on tehty kuluttajansuojalaissa (38/1978) kuluttajaluottosopimusten osalta. Kuluttajansuojalain 7 luvun 15 §:n mukaan luotonantajan on ennen kuluttajaluottosopimuksen tekemistä todennettava luottoa hakevan henkilöllisyys huolellisesti. Jos henkilöllisyys todennetaan sähköisesti, luotonantajan on ensitunnistamisvaiheessa käytettävä tunnistusmenetelmää, joka täyttää vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 8 §:ssä säädetyt vaatimukset. Tämä tarkoittaa käytännössä sitä, että sähköisessä ympäristössä tunnistamisen tulisi tapahtua esimerkiksi verkkopankkitunnuksilla tai teleyritysten mobiilivarmenteilla. Kuluttajansuojalain säännökset henkilöllisyyden todentamisesta eivät koske hyödykesidonnaisia kertaluottoja tai laskutuspalveluja, joita tyypillisesti tarjotaan rahoitusvaihtoehdoksi verkkokaupassa.

Lisäksi esimerkiksi 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.

Maksupalvelulain 85 c §:n mukaan vahvaa tunnistamista on käytettävä muun muassa, jos maksaja käyttää maksutiliään tietoverkon välityksellä tai käynnistää sähköisen maksutapahtuman.

Asiakkaan tunnistaminen on olennaista myös telealan tietoturvasääntelyn sekä rahanpesun ja terrorismin rahoittamisen estämistä koskevan sääntelyn toteuttamisessa. Etenkin rahanpesun estämistä koskeva sääntely vaikuttaa laajasti eri toimialoilla, kuten finanssialalla, tilintarkastuksessa ja kiinteistönvälityksessä.

Vaikka lainsäädännöstä ei seuraisi velvoitetta sopimusta sähköisesti tehtäessä käyttää vahvaa tunnistamista, on sopimusosapuolen, erityisesti elinkeinonharjoittajan omassa intressissä, että hän oikeustoimen laatu ja muut olosuhteet huomioon ottaen riittävän luotettavasti varmistuu sopimuskumppaninsa henkilöllisyydestä. Sopimusoikeudessa lähtökohtana on, että sopimukseen vetoavan on näytettävä toteen sopimuksen syntymiseen vaadittavat tosiseikat, kuten sopimuksen solmiminen.

Syytä on kiinnittää huomiota myös siihen, että vahvaa sähköistä tunnistamista koskeva vaatimus ei tarkoita sitä, että sopimus olisi tehtävä tietyssä muodossa, kuten kirjallisesti, taikka että sen laiminlyönnistä seuraisi automaattisesti lain nojalla se, ettei sopimus sido. Kyse ei ole siis lainsäädännössä joidenkin (harvalukuisten) oikeustoimien tekemiselle asetetusta ns. varsinaisesta muotovaatimuksesta. Vahvan sähköisen tunnistamisen laiminlyömisestä voi kuitenkin seurata sanktio, esim. kuluttajansuojalain 7 luvussa säädetyn velvoitteen rikkomisesta voidaan määrätä luotonantajalle seuraamusmaksu.

2.4. Henkilötunnuksen muuttamisen hyödyt ja haitat

Yksilön suojaamisen ja aseman kannalta henkilötunnuksen muuttamisella identiteettivarkaustilanteessa on sekä hyötyjä että haittoja. Hyödyt liittyvät yksityisyyden suojan parantamiseen ja mahdollisten henkilötunnuksen avulla tehtävien myöhempien rikosten ehkäisemiseen. Haitat kytkeytyvät hallinnolliseen ja myös taloudelliseen taakkaan, mikä henkilötunnuksen muuttamisesta aiheutuu yksilölle.

Sellaisissa laajamittaisissa tietoturvaloukkauksissa tai tietomurroissa, joissa henkilötietoja on vuotanut tunnistetietojen lisäksi, rikoksen uhrien yksityisyyden loukkaus aiheutuu ennen muuta muista sivullisen tietoon joutuneista tiedoista kuin henkilötunnuksesta. Henkilötunnuksen muuttamisella ei vaikuteta näiden tietojen lainvastaiseen käsittelyyn.

Henkilötunnuksen muuttaminen ei myöskään aukottomasti poista petosten tekomahdollisuutta varastetulla identiteetillä. Toimija, joka ei noudata hyviä käytäntöjä ja luottaa vain henkilön itsensä ilmoittamiin tietoihin, ei myöskään todennäköisesti tarkista henkilötunnuksen voimassaoloa väestötietojärjestelmästä. Näin ollen petosten tekeminen myös vanhalla henkilötunnuksella voi jatkua. Identiteettirikoksia ja vahinkoa, myös petoksia, voi toteuttaa myös muiden henkilötietojen, kuten nimen, osoitteen, sähköpostin tai puhelinnumeron avulla.

Henkilötunnuksen muuttamisella voidaan edellä mainittuja väärinkäytöksiä jossain määrin rajoittaa, mutta ei kuitenkaan täysin ehkäistä. Laaja-alaisen tietoturvaloukkauksen tai tietomurron yhteydessä tekijällä tai sillä, joka tällaisen tietovuodon johdosta on saanut käsiinsä henkilötietoja, mukaan lukien henkilötunnuksen, on saamiensa tietojen perusteella mahdollista saada uusikin

henkilötunnus tietoonsa verrattaen helposti, koska väärinkäyttäjällä on jo valmiiksi tiedossa henkilön syntymäaika ja sukupuoli vanhan henkilötunnuksen perusteella. Henkilötunnus ei ole salassa pidettävä tieto, vaan sitä käytetään laajasti yhteiskunnan eri toiminnoissa.

2.5. Tieto- ja viestintärikoksia koskeva sääntely

Tieto- ja viestintärikoksia koskevat rangaistussäännökset ovat rikoslain 38 luvussa. Luvun mukaan rangaistavia rikoksia ovat salassapitorikos, salassapitorikkomus, viestintäsalaisuuden loukkaus, törkeä viestintäsalaisuuden loukkaus, tietoliikenteen häirintä, törkeä tietoliikenteen häirintä, lievä tietoliikenteen häirintä, tietojärjestelmän häirintä, törkeä tietojärjestelmän häirintä, tietomurto, törkeä tietomurto, suojauksen purkujärjestelmärikos, tietosuojarikos ja identiteettivarkaus.

Tieto- ja viestintärikoksia koskevia rikoslain 38 luvun säännöksiä täydennettiin ja muutettiin viimeksi merkittävästi vuonna 2015, kun lainsäädäntö saatettiin vastaamaan vaatimuksia, jotka johtuivat tietojärjestelmiin kohdistuvia hyökkäyksiä koskevasta direktiivistä 2013/40/EU. Tuolloin muun ohessa korotettiin tietomurron ja törkeän tietomurron enimmäisrangaistuksia, lisättiin tekotapoja useisiin luvun rikoksiin ja säädettiin uutena rikoksena rangaistavaksi identiteettivarkaus.

Direktiivin ja samalla tuolloin tehtyjen lainsäädäntömuutosten taustalla oli direktiivin johdantokappaleiden mukaan se, että tietojärjestelmiä vastaan tehdyt hyökkäykset ovat kasvava uhka maailmanlaajuisesti. Elintärkeitä tietojärjestelmiä vastaan pyritään tekemään entistä vaarallisempia ja toistuvia laajamittaisia hyökkäyksiä. Laajamittaiset verkkohyökkäykset voivat aiheuttaa merkittäviä taloudellisia vahinkoja keskeyttämällä tietotietojärjestelmät ja viestinnän sekä aiheuttamalla kaupallisesti tärkeiden luottamuksellisten tietojen tai muun datan menetyksen tai muuttumisen. Tuossa yhteydessä korostettiin myös identiteettivarkauden ja muiden henkilöllisyyteen liittyvien rikosten estämistä. Rikoslakiin tehtävillä muutoksilla laajennettiin sähköisessä muodossa olevan tiedon ja tiedonvälityksen rikosoikeudellista suojaa, ja lainsäädännön lähentämisen Euroopan unionin jäsenvaltioiden välillä arvioitiin jossakin määrin edes-auttavan Suomen viranomaisten mahdollisuuksia parantaa yhteistyön edellytyksiä rajat ylittävien rikosten selvittämisessä.

Yleisesti ottaen tekninen kehitys on lisännyt tietoverkkoon ja sähköiseen viestintään kohdistuvien laajamittaisten rikosten tekemisen mahdollisuutta rikostentekijöiden teknisen osaamisen ja järjestelmien suojausten asettamissa rajoissa. Tällaisesta rikollisuudesta on tullut myös yhä enemmän rajat ylittävää rikollisuutta, jonka selvittämiseksi myös todistusaineistoa on hankittava toisista valtioista.

2.6. Sääntelyn arviointi

Käsillä oleva tietomurtotapaus on nostanut esiin sen, ettei henkilötunnuksia voida muuttaa tietoturvaloukkauksien tai tieto- ja viestintärikosten yhteydessä ennakollisena yksilöitä suojaavana toimenpiteenä. Voidaan katsoa, että käsillä oleva laajaksi arvioitava rikos on tuonut esiin tarpeen arvioida henkilötunnuksen muuttamisen sääntelymuutostarpeita yhteiskuntakehityksestä johtuvista syistä. Yhteiskunta on kehittynyt merkittävästi digitaalisemmaksi viimeisen kymmenen vuoden aikana. Yksilön oikeuksien loukkauksia on laajasti mahdollista tehdä sähköisten asiointipalvelujen avulla ja internetissä yleisesti. VTJ-lain

säätämisen aikaan rikollisin keinoin haltuun saatujen henkilötunnusten avulla tehtävät muut rikokset ovat olleet harvinaisempia ja suppeampia. Esimerkiksi identiteettivarkaus kriminalisoitiin erikseen vasta 2015. Myös kiristystarkoituksissa tehdyt rikokset ovat uudehko ilmiö. Digitalisaation ja yhteiskunnan kehitys on mahdollistanut laajempia ja yleisesti vahingollisempia tieto- ja viestintärikoksia, joita ei ole tässä mittakaavassa voitu huomioida VTJ-lain säätämisen yhteydessä.

3. Sääntelyvaihtoehdot

3.1. Yleisesti sääntelyvaihtoehdoista

Sääntelymuutokseen, joka mahdollistaisi henkilötunnuksen muuttamisen tietojen hyväksikäyttöön liittyvien väärinkäytösten johdosta, liittyy useita arvioitavia asioita. Tällaisen sääntelymuutoksen valmistelussa on otettava huomioon esimerkiksi henkilötunnuksen pysyvä luonne ja merkitys henkilön oikeusasemalle, olemassa olevan sääntelyn tyhjentävä ja poikkeuksellinen luonne, viranomaisten mahdollisuudet ja toimivalta arvioida tapahtuneen loukkauksen lainvastaisuutta sekä käytännön vaikutukset ja hyödyt henkilötunnuksen muuttamisesta. Mikäli nämä näkökohdat otetaan huomioon, on tässä muistiossa esitetyn alustavan arvion pohjalta kuitenkin tunnistettu mahdollisia tapoja säätää henkilötunnuksen muuttamisesta väärinkäytöksen seurauksena ennaltaehkäisevästi.

Keskeistä on, että tunnuksen muuttamisen tulisi aina tapahtua henkilön omasta hakemuksesta. Henkilötunnus on keskeinen henkilön identiteetille ja oikeusasemalle, eikä sitä tulisi muuttaa viranomaisaloitteisesti. Tätä puoltaa myös se, että sääntelyn tarkoituksena olisi ehkäistä henkilölle itselleen aiheutuvia haittoja. Henkilö itse on parhaassa asemassa arvioimaan sen, ovatko haitat sellaisia, että tunnuksen muuttamisesta aiheutuvat vaikutukset ja kustannukset ovat hänen kohdallaan perusteltuja.

Päätöksen henkilötunnuksen muuttamisesta tekisi aina Digi- ja väestötietovirasto. Päätökseen johtavasta menettelystä voitaisiin kuitenkin säätää eri tavoin. Olennaista on esimerkiksi, tehtäisiinkö jokaisen hakemuksen kohdalla erillinen arvio siitä, onko tapahtunut riittävän vakava loukkaus ja siitä, onko tunnuksen muuttaminen kyseisessä tapauksessa tarkoituksenmukainen keino ehkäistä loukkauksesta aiheutuvia haittoja. Mahdollista olisi myös säätää kaksivaiheisesta menettelystä, jossa Digi- ja väestötietovirasto voisi ensi vaiheessa todeta yleisesti edellytysten täyttymisen ja toisessa vaiheessa arvioida yksittäisten hakemusten kohdalla vain henkilön asianosaisasemaan perustuvan oikeuden tunnuksen muuttamiseen.

Uutta sääntelyä valmisteltaessa on huomioitava, että voimassa oleva sääntely VTJ-lain 12 §:ssä on tarkoitettu sekä tyhjentäväksi että vain erityisen poikkeuksellisissa tapauksissa sovellettavaksi. Lainsäätäjä on siis tarkoittanut pykälän ainoaksi henkilötunnuksen muuttamista koskevaksi säännökseksi, jonka soveltamiskynnys on korkea. Tästä näkökulmasta uuden pykälän säätämistä ilman, että lainsäätäjä ottaa kantaa myös voimassa olevan pykälän luonteeseen, voidaan pitää ongelmallisena.

Seuraavaksi kuvataan kaksi erilaista vaihtoehtoa säädösmuutoksiksi. Luonnoksiin sisältyviä ratkaisuja yhdistelemällä on mahdollista toteuttaa myös näistä poikkeavia säädösehdotuksia. Molempia vaihtoehtoja tarkasteltaessa on myös huomattava, että ne ovat vasta alustavia

ehdotuksia. Luonnosten yhteydessä on nostettu esiin alustavasti tunnistettuja ongelmia ja lisäselvitystarpeita.

3.2. Vaihtoehto 1: Kaksivaiheinen menettely tietoturvaloukkauksen johdosta

Vaihtoehdossa 1 eriytettäisiin yksittäistapauksissa tapahtuva henkilötunnuksen muuttaminen, joka tapahtuisi jo voimassa olevin edellytyksin lain 12 §:n mukaisesti, ja useita henkilöitä koskettavan tietoturvaloukkauksen yhteydessä tapahtuva henkilötunnuksen muuttaminen, jota koskisi kokonaan uusi sääntely 12 a §:ssä. Voimassa olevaa pykälää, siihen tehtävine muutoksineen, ja uutta pykälää olisi luettava yhtenäisenä kokonaisuutena.

Vaihtoehto 1 perustuisi tietosuojalainsäädännön mukaiselle henkilötietojen tietoturva-loukkaukselle, jonka tietoon saatuaan rekisterinpitäjä tekee arvioinnin loukkauksen ilmoittamisesta tietosuojavaltuutetulle ja rekisteröidyille yleisen tietosuoja-asetuksen tai henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018) mukaisesti. Rekisterinpitäjän on tehtävä arviointi loukkauksen ilmoittamisesta tietosuojavaltuutetulle ja rekisteröidyille, kun se saa loukkauksen tietoonsa. Tarkastelu kohdistuisi ensi vaiheessa tähän tietoturvaloukkaukseen kokonaisuutena ja siihen, voidaanko henkilötunnusten muuttamisella kyseisessä tapauksessa estää väärinkäytöksistä aiheutuvia haittoja. Digi- ja väestötietovirasto tekisi erillisen päätöksen siitä, toteutuvatko henkilötunnuksen muuttamista koskevat yleiset edellytykset kyseisen tietoturvaloukkauksen kohdalla ja tämä päätös toimisi perustana yksittäisille henkilötunnusten muuttamista koskeville hakemuksille. Mikäli yleisten edellytysten olisi tietoturvaloukkauksen osalta todettu täyttyvän, tehtäisiin päätös yksittäistapauksessa ainoastaan henkilön asianosaisasemaa koskevan arvion pohjalta.

Muutettavat tai uudet lainkohdat on merkitty kursiivilla.

12 §

Henkilötunnuksen korjaaminen ja muuttaminen *yksittäistapauksessa*

Väestötietojärjestelmään talletettu henkilötunnus on korjattava, jos tunnus on teknisesti virheellinen tai tieto tunnukseen sisältyvästä syntymäajasta tai sukupuolesta on virheellinen. Korjaamisesta päättää Digi- ja väestötietovirasto. Digi- ja väestötietoviraston on varattava sille henkilölle, jota asia koskee, tai hänen lailliselle edustajalleen tilaisuus lausua mielipiteensä asiasta. Korjaamisesta on ilmoitettava edellä mainitulle henkilölle.

Väestötietojärjestelmään talletettu henkilötunnus voidaan *yksittäistapauksessa* muuttaa, jos:

1) muuttaminen on ehdottoman välttämätöntä henkilön suojelemiseksi sellaisissa tilanteissa, joissa hänen terveyteensä tai turvallisuuteensa kohdistuu ilmeinen ja pysyvä uhka;

2) muu kuin henkilötunnuksen haltija on toistuvasti väärinkäyttänyt tunnusta ja käytöstä on aiheutunut merkittävää taloudellista tai muuta haittaa tunnuksen oikealle

haltijalle ja henkilötunnuksen muuttamisella voidaan tosiasiallisesti estää väärinkäytön haitallisten seurausten jatkuminen;

3) henkilö on transseksuaalin sukupuolen vahvistamisesta annetun lain (563/2002) mukaisesti vahvistettu vastakkaiseen sukupuoleen kuuluvaksi.

Henkilötunnuksen muuttamisesta *yksittäistapauksessa* päättää 2 momentin 1 ja 2 kohdassa tarkoitetussa tapauksessa Digi- ja väestötietovirasto ja 3 kohdassa tarkoitetussa tapauksessa transseksuaalin sukupuolen vahvistamisesta annetun lain 3 §:ssä tarkoitettu viranomainen. Asianosaisen on haettava henkilötunnuksen muuttamista kirjallisesti.

12 a §

Henkilötunnuksen muuttaminen tietoturvaloukkauksen seurauksena

Henkilötunnus voidaan muuttaa tietoturvaloukkauksen seurauksena, jos:

1) henkilötunnuksia sisältävään rekisteriin on kohdistunut yleisen tietosuoja-asetuksen 4 artiklan 1 kohdan 12 alakohdan tai henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain

(1054/2018) 3 §:n 1 momentin 9 kohdan tarkoittama henkilötietojen tietoturvaloukkaus, joka aiheuttaa rekisterinpitäjän arvion mukaan todennäköisesti merkittävän riskin luonnollisten henkilöiden oikeuksille ja vapauksille;

2) tietoturvaloukkaukseen sisältyvä tietojen luvaton luovuttaminen taikka pääsy tietoihin merkitsee korkealla todennäköisyydellä, että rekisteriin sisältyneitä henkilötunnuksia on laittomasti kolmansien osapuolten hallussa ja niitä tullaan hyödyntämään rikollisessa tarkoituksessa;

3) henkilötunnusten muuttamisella voidaan tosiasiassa ehkäistä tietoturvaloukkauksesta aiheutuvia haitallisia seurauksia; ja

4) asianosainen hakee henkilötunnuksen muuttamista.

Rekisterinpitäjän ja tietosuojavaltuutetun on toimitettava Digi- ja väestötietovirastolle tarvittavat tiedot sen arvioimiseksi, täyttyvätkö 1 momentin 1-3 kohdassa asetetut yleiset edellytykset henkilötunnuksen muuttamiseksi todetun tietoturvaloukkauksen osalta. Digi- ja väestötietoviraston on tehtävä erillinen päätös yleisten edellytysten täyttymisestä.

Digi- ja väestötietovirasto päättää henkilötunnuksen muuttamisesta tietoturvaloukkauksen seurauksena. Henkilötunnuksen muuttamista on haettava kirjallisesti ja hakemuksesta on käytävä ilmi henkilön asianosaisasema tietoturvaloukkauksessa. Mikäli yleisten edellytysten on 2 momentin mukaisesti todettu täyttyvän ja Digi- ja

väestötietovirasto pitää henkilön asianosaisasemaa ilmeisenä, sen on muutettava henkilötunnus.

Vaihtoehto 1 edellyttäisi vielä lisäselvitystä erityisesti seuraavista näkökohdista:

- Valmistelussa olisi arvioitava tarkemmin yhdenvertaisuusnäkökohtia ja sitä, missä määrin todetun tietoturvaloukkauksen johdosta tehtävä henkilötunnuksen muutos on perusteltavissa suhteessa yksittäistapauksiin, joissa vahingon riski olisi samankaltainen.

- Suhde tietosuojasääntelyssä määriteltävään tietoturvaloukkaukseen ja sen riskien arviointiin edellyttää tarkennusta lainsäädännön systematiikan osalta. Valmistelun kuluessa ei ole kyetty kattavasti arvioimaan säännöksen suhdetta yleiseen tietosuoja-asetukseen, tietosuojalakiin tai henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettuun lakiin.

- Vaihtoehtoon sisältyy riski siitä, että henkilötietojen käsittelijä, rekisterinpitäjä tai muu henkilötietojen käsittelyyn liittyvä taho ei arvioi loukkauksen luonnetta oikein tai jättää ilmoittamatta loukkauksesta. Myös tietosuojavaltuutetun tiedonsaanti perustuu asianosaisten ilmoitukseen. Toisaalta Digi- ja väestötietoviraston mahdollisuudet itsenäisesti todeta loukkauksen tapahtuminen tai arvioida sen merkittävyyttä ovat rajalliset.

- Eri viranomaisten toimivaltuuksia ja toimijoiden välisiä tiedonsaanti-oikeuksia olisi arvioitava tarkemmin. Oikeusministeriön hallinnonalan näkökulmasta on olennaista, että valmistelussa arvioitaisiin huolellisesti muutoksen vaikutukset tietosuojavaltuutettuun.

- Sääntely edellyttäisi Digi- ja väestötietovirastolta arviota siitä, millainen henkilötunnuksen väärinkäytön riski todetusta tietoturvaloukkauksesta aiheutuu. Arvion perusteita ja menettelyitä olisi tarkennettava.

- Valmistelussa olisi selvitettävä tarkemmin, tulisiko oikaisuvaatimus- ja valitusoikeuksista säätää erikseen ja millä tahoilla olisi oikeus vaatia oikaisua tai valittaa yleisiä edellytyksiä koskevasta päätöksestä (asianosaiset, rekisterinpitäjä, tietosuojavaltuutettu, muut tahot).

- Säännöksen vaikuttavuus riippuisi olennaisesti siitä, mitä säännöksen toimeenpano käytännössä edellyttäisi ja se, millaisella aikataululla muutosta koskevat hakemukset saataisiin vireille ja käsiteltyä.

3.3. Vaihtoehto 2: Yksivaiheinen menettely tietomurron johdosta

Vaihtoehdossa 2 muutettaisiin lain 12 §:ää kokonaisuudessaan niin, että siihen lisättäisiin uusi mahdollisuus muuttaa henkilötunnus tietomurtorikoksen seurauksena. Perusteena säännöksen

muuttamiselle ei tässä vaihtoehdossa olisi useaa henkilöä koskeva todettu loukkaus, jota voitaisiin käsitellä kokonaisuutena, vaan yksittäiselle henkilölle rikoksesta johtuva ilmeinen riski henkilötunnuksen rikollisesta käytöstä. Väärinkäyttötilanteissa yksilön henkilötunnus voitaisiin siis muuttaa yhtäältä siitä syystä, että toistuvaa haitallista väärinkäyttöä on jo tapahtunut (voimassa oleva peruste), ja toisaalta ennaltaehkäisevästi, kun loukkaus on selkeästi todettavissa ja riski on olosuhteisiin nähden ilmeinen (uusi peruste).

Vaihtoehdossa 2 tunnuksen muuttaminen perustuisi tietosuojalainsäädännössä tarkoitetun henkilötietojen tietoturvaloukkauksen toteamisen sijaan rikosoikeudellisen tietomurron tai törkeän tietomurron tapahtumiselle. Tässä vaihtoehdossa olennaista on, mistä rikoksen tapahtuminen tai epäily todetaan – tätä olisi selvitettävä tarkemmin. Luonnostellussa vaihtoehdossa 2 tätä edellytystä ei ole selkeästi kuvattu pykälätekstissä, mutta tarkastelu voisi perustua esimerkiksi esitutkinnan käynnistämiseen tai rikosasiassa annettuun tuomioon. Digi- ja väestötietoviraston itsenäistä arviota rikoksen tunnusmerkistöstä ei kuitenkaan voida pitää tarkoituksenmukaisena.

Vaihtoehdossa 2 henkilötunnuksen muuttamista koskeva menettely olisi yksivaiheinen. Digi- ja väestötietovirasto arvioisi edellytysten olemassaolon kokonaisuudessaan jokaisen yksittäisen hakemuksen kohdalla. Vaihtoehtoon sisältyy myös säännös Digi- ja väestötietoviraston neuvontavelvoitteesta sen varmistamiseksi, että henkilötunnusta ei muuteta turhaan ja että hakija ymmärtää muuttamisen seuraukset**.**

Muutettavat tai uudet lainkohdat on merkitty kursiivilla.

12 §

Henkilötunnuksen korjaaminen ja muuttaminen

Väestötietojärjestelmään talletettu henkilötunnus on korjattava, jos tunnus on teknisesti virheellinen tai tieto tunnukseen sisältyvästä syntymäajasta tai sukupuolesta on virheellinen. Korjaamisesta päättää Digi- ja väestötietovirasto. Digi- ja väestötietoviraston on varattava sille henkilölle, jota asia koskee, tai hänen lailliselle edustajalleen tilaisuus lausua mielipiteensä asiasta. Korjaamisesta on ilmoitettava edellä mainitulle henkilölle.

Väestötietojärjestelmään talletettu henkilötunnus voidaan muuttaa, jos:

1) muuttaminen on ehdottoman välttämätöntä henkilön suojelemiseksi sellaisissa tilanteissa, joissa hänen terveyteensä tai turvallisuuteensa kohdistuu ilmeinen ja pysyvä uhka;

2) henkilötunnus on rikoslain (39/1889) 38 luvun 8 ja 8 a §:ssä tarkoitetun tietomurron tai törkeän tietomurron seurauksena kolmannen osapuolen tiedossa siten, että jo tehdyiksi epäiltyjen rikosten tai muuten olosuhteiden perusteella on ilmeistä, että henkilötunnusta tullaan käyttämään rikollisiin tarkoituksiin, ja henkilötunnuksen muuttamisella voidaan suurella todennäköisyydellä ehkäistä tietomurrosta tai törkeästä tietomurrosta aiheutuvia haitallisia seurauksia.

3) muu kuin henkilötunnuksen haltija on toistuvasti väärinkäyttänyt tunnusta ja käytöstä on aiheutunut merkittävää taloudellista tai muuta haittaa tunnuksen oikealle haltijalle ja henkilötunnuksen muuttamisella voidaan tosiasiallisesti estää väärinkäytön haitallisten seurausten jatkuminen;

4) henkilö on transseksuaalin sukupuolen vahvistamisesta annetun lain (563/2002) mukaisesti vahvistettu vastakkaiseen sukupuoleen kuuluvaksi

Henkilötunnuksen muuttamisesta päättää 2 momentin *1-3 kohdassa* tarkoitetussa tapauksessa Digi- ja väestötietovirasto ja 4 kohdassa tarkoitetussa tapauksessa transseksuaalin sukupuolen vahvistamisesta annetun lain 3 §:ssä tarkoitettu viranomainen. Asianosaisen on haettava henkilötunnuksen muuttamista kirjallisesti.

Digi- ja väestötietoviraston on 2 momentin 1-3 kohdassa tarkoitetuissa tilanteissa annettava hakijalle tarvittavat tiedot henkilötunnuksen muuttamisen vaikutuksista ennen henkilötunnuksen muuttamista.

Vaihtoehto 2 edellyttäisi vielä lisäselvitystä erityisesti seuraavista näkökohdista:

- Luonnoksessa henkilötunnuksen muuttaminen on kiinnitetty tietomurtoon tai törkeään tietomurtoon. Valmistelussa olisi kuitenkin edelleen harkittava, jäisikö soveltamisalan ulkopuolelle tapauksia, joissa tosiasiassa henkilölle aiheutuva haitta on vastaava, vaikka henkilötunnus on päätynyt sivullisen haluun muulla tavoin. Kysymystä olisi arvioitava myös yhdenvertaisuuden näkökulmasta.

- Digi- ja väestötietovirasto ei alustavan näkemyksen mukaan voi itsenäisesti arvioida rikosepäilyn todennäköisyyttä tai rikostunnusmerkistön täyttymistä. Edellytysten täyttyminen olisi sidottava esimerkiksi esitutkinnan käynnistymiseen tai muuhun objektiiviseen tapahtumaan ja sääntelyvaihtoehtoja olisi tältä osin arvioitava tarkemmin. Arvio vaikuttaa olennaisesti myös siihen, kuinka laajassa mittakaavassa henkilötunnuksia tulisi muutettavaksi ja voidaanko toimenpiteellä tosiasiassa ehkäistä tietomurron haitallisia vaikutuksia henkilötunnuksen väärinkäytön osalta.

- Valmistelussa olisi selvitettävä tarkemmin, edellyttääkö menettely erityisiä tiedonsaantioikeuksia ja millä tavoin Digi- ja väestötietovirasto saa tiedon edellytysten arvioimiseksi.

- Säännöksen vaikuttavuus riippuisi olennaisesti siitä, mitä säännöksen toimeenpano käytännössä edellyttäisi ja se, millaisella aikataululla muutosta koskevat hakemukset saataisiin vireille ja käsiteltyä.

3.4. Perustuslaillisista näkökohdista

3.4.1. Henkilötunnus turvaa henkilön oikeuksia ja velvollisuuksia

Henkilötunnus on tarkoitettu pysyväksi ja sen avulla varmistetaan henkilöiden yksilöitävyys. Henkilötunnus ja sen käsittely ovat tästä näkökulmasta merkityksellisiä myös perustuslaissa turvattujen perusoikeuksien toteuttamiselle. Henkilötunnuksen merkitys yksilön asemalle ja yhteiskunnalle tulisi huomioida valmisteltaessa siihen kohdistuvia lainsäädäntömuutoksia.

Henkilötunnuksen yksilöllisyys ja sen merkitys yksilön oikeuksien ja velvollisuuden toteuttamisen perustana merkitsee myös sitä, ettei perusoikeuksien toteuttamisen näkökulmasta, voi syntyä tilannetta, ettei henkilölle, jolle lainsäädännön mukaan on myönnettävä henkilötunnus, ei sitä voitaisikaan myöntää yksilöivien tunnusten loppumisen vuoksi.

3.4.2. Yhdenvertaisuus

Perustuslain 6 §:ssä säädetään yhdenvertaisuudesta. Säännöksen mukaan ihmiset ovat yhdenvertaisia lain edessä eikä ketään saa ilman hyväksyttävää perustetta asettaa eri asemaan sukupuolen, iän, alkuperän, kielen, uskonnon, vakaumuksen, mielipiteen, terveydentilan, vammaisuuden tai muun henkilöön liittyvän syyn perusteella.

Yleinen yhdenvertaisuuslauseke kohdistuu myös lainsäätäjään. Lailla ei voida ilman yleisesti hyväksyttävää perustetta eli mielivaltaisesti asettaa ihmisiä tai ihmisryhmiä toisia edullisempaan tai epäedullisempaan asemaan. Yhdenvertaisuusnäkökohdilla on merkitystä sekä myönnettäessä lailla etuja ja oikeuksia että asetettaessa velvollisuuksia.

Yhdenvertaisuus ei kuitenkaan merkitse kaikkien ihmisten kaikissa suhteissa samanlaista kohtelua, elleivät asiaan vaikuttavat olosuhteet ole samanlaisia. Lainsäädännölle on ominaista, että siinä kohdellaan tietyn hyväksyttävän yhteiskunnallisen intressin vuoksi ihmisiä eri tavoin muun muassa tosiasiallisen tasa-arvon edistämiseksi. (HE 309/1993 vp, s. 42–43, PeVL 45/2016 vp, PeVL 67/2014 vp, PeVL 31/2014 vp, PeVL 38/2006 vp, s. 2) Perustuslakivaliokunta onkin vakiintuneesti todennut, ettei yleisestä yhdenvertaisuusperiaatteesta johdu tiukkoja rajoja lainsäätäjän harkinnalle pyrittäessä kulloisenkin yhteiskuntakehityksen vaatimaan sääntelyyn. (PeVL 11/2012 vp, s. 2, PeVL 2/2011 vp, s. 2, PeVL 64/2010 vp, s. 2, PeVL 35/2010 vp, s. 2, PeVL 5/2008 vp, s. 5, PeVL 38/2006 vp, s. 2, PeVL 1/2006 vp, s. 2, PeVL 15/2001 vp, s. 3)

Keskeistä lainsäädännön arvioinnissa on, voidaanko kulloisetkin erottelut perustella perusoikeusjärjestelmän kannalta hyväksyttävällä tavalla. (PeVL 75/2014 vp, PeVL 67/2014 vp, PeVL 31/2014 vp, PeVL 46/2006 vp, s. 2, PeVL 16/2006 vp, s. 2, PeVL 73/2002 vp) Perustuslakivaliokunta on eri yhteyksissä johtanut perustuslain yhdenvertaisuussäännöksistä vaatimuksen, että erottelut eivät saa olla mielivaltaisia eivätkä ne saa muodostua kohtuuttomiksi. (PeVL 47/2018 vp, PeVL 20/2017 vp, PeVL 58/2014 vp, PeVL 7/2014 vp, s. 5–6, PeVL 11/2012 vp, s. 2, PeVL 37/2010 vp, s. 3, PeVM 11/2009 vp, s. 2, PeVL 18/2006 vp, s. 2.)

Ehdotusta muuttaa henkilötunnuksen muuttamista koskevaa säännöstä erityisesti käsillä olevan laajan tietomurron aiheuttamassa tilanteessa on arvioitava edellä mainittujen tekijöiden valossa. Käsillä oleva tilanne on nostanut esiin sen, ettei nykyinen lainsäädäntö mahdollista tunnuksen muuttamista ennakollisena yksilöitä suojaavana toimenpiteenä laajoissakaan tietoturvaloukkauksissa tai tietomurroissa, joihin sisältyy ilmeinen riski laajasta väärinkäytöstä. Yhteiskunta on kehittynyt merkittävästi digitaalisemmaksi viimeisen kymmenen vuoden aikana. Yksilön oikeuksien loukkauksia on mahdollista tehdä sähköisien asiointipalvelujen avulla ja internetissä yleisesti huomattavasti aiempaa laajemmin. Loukkaustilanteet voivat myös kehittyä hyvin nopeasti ja aiheuttaa henkilöille laajamittaisia vahinkoja. Henkilötunnuksen muuttamisen sääntely, joka edellyttää jälkikäteistä toistuvan ja merkittävän vahingon osoittamista, vastaa huonosti nyky-yhteiskunnan haasteisiin. Voidaan katsoa, että käsillä oleva laajaksi arvioitava rikos on nostanut esiin tarpeen muuttaa sääntelyä yhteiskuntakehityksestä johtuvista syistä.

Lainsäädännön yhdenvertaisuuden näkökulmasta on kuitenkin varmistettava, että ihmisiä kohdellaan eri tavoin vain siltä osin, kuin se on yhteiskunnallisen intressin vuoksi hyväksyttävää ja että tämä erottelu voidaan perustella perusoikeusjärjestelmän kannalta hyväksyttävällä tavalla. Tästä näkökulmasta on katsottava, ettei tiettyyn yksittäiseen rikoksen tai tiettynä ajankohtana tapahtuneiden rikosten uhreja ei lähtökohtaisesti tulisi kohdella eri tavoin kuin muita vastaavan rikoksen uhreja. Henkilötunnuksen väärinkäyttöön liittyvät riskit ja siitä aiheutuvat vahingot ovat yksilön aseman ja oikeuksien näkökulmasta vastaavia riippumatta rikoksen laajuudesta tai ajankohdasta. Valmistelussa voidaan kuitenkin arvioida vielä tarkemmin sitä, liittyykö rikoksen vakavuuteen tai laajuuteen tekijöitä, jotka olennaisesti vaikuttaisivat erilaisen kohtelun hyväksyttävyyteen.

Yhdenvertaisuuden vaatimus vaikuttaa myös lain ajalliseen soveltamiseen, jota voidaan arvioida sekä taaksepäin että eteenpäin. Ehdotettu muutostarve on noussut esiin nopealla aikataululla hyvin laajamittaisen epäillyn tietomurtorikoksen johdosta. Lain valmistelussa olisi kuitenkin varmistettava, että mahdollisesti aiemmin vastaavan rikoksen uhreiksi joutuneita ei aseteta lainsäädännössä eriarvoiseen asemaan, mikäli vaikutukset yksilön asemaan olisivat vastaavat. Tästä näkökulmasta henkilötunnuksen muuttamista koskevia uusia säännöksiä olisi sovellettava objektiivisin kriteerein myös suhteessa aiemmin tapahtuneisiin loukkauksiin.

Tästä näkökulmasta olisi tarkasti arvioitava myös säännöksen mahdollista määräaikaisuutta. Ellei lainsäädäntöön tai toimintatapoihin kohdistettaisi laajempia uudistuksia, jotka tekisivät nyt ehdotettavat muutokset tarpeettomiksi määräajan kuluttua, on olemassa riski siitä, että määräaikaisuus erottelisi ihmisiä mielivaltaisin perustein. Henkilön aseman ja loukkauksesta aiheutuvien vahinkojen näkökulmasta ei voida katsoa, että tapahtuma-ajankohta olisi yhteiskunnallisesti hyväksyttävä erotteluperuste.

Yllä kuvatuin perustein on katsottava, että henkilötunnuksen muuttamisen mahdollistaminen vain tietyn loukkauksen uhriksi joutuneille taikka tilapäisesti määräajaksi on yhdenvertaisuuden näkökulmasta ongelmallista. On olemassa riski siitä, että lainsäätäjä asettaisi ihmiset eriarvoiseen asemaan ilman objektiivisesti hyväksyttävää perustetta. Tällä tavalla rajoitetut säännökset olisi arvioitava hyvin tarkasti perustuslaillisesta näkökulmasta.

4. Vaikutukset

4.1. Vaikutukset identiteettivarkauksien ja muiden rikollisissa tarkoituksessa tehtävien tekojen ehkäisyyn

Mahdollisen henkilötunnuksen muuttamista koskevan muutoksen vaikutukset pitäisi arvioida ja punnita sillä saatavan yhteiskunnallisen ja yksilöille saatavan hyödyn näkökulmasta ja toisaalta siitä näkökulmasta, minkälaisia muita negatiivisiakin vaikutuksia asianosaisten asemaan muutoksilla mahdollisesti olisi. Henkilötunnuksen muuttamista koskevan sääntelyn tarkastelun kannalta on arvioitava sitä, onko nimenomaan henkilötunnuksen avulla tehtävien rikosten tai muiden asianosaista haittaavien tekojen riski tai vaikutukset niin merkittäviä, että henkilötunnuksen muuttaminen olisi sen muuttamisesta aiheutuviin haittoihin nähden vaikuttavaa ja yksilön aseman kannalta hyödyllistä. Henkilötunnuksen muuttamisen hyötyjä ja haittoja on käsitelty kappaleessa 2.4.

Kolmannen osapuolen haltuun joutuneella henkilötunnuksella voidaan aiheuttaa jossain määrin vahinkoja tai oikeudenloukkauksia asianosaiselle. Henkilö voi erilaisilla toimilla, kuten kielloilla ja estoilla suojautua väärinkäytöksiltä. Henkilötunnuksen tai muiden henkilötietojen vääriin käsiin joutumisen taustalla ei välttämättä ole tietoverkkorikosta. Tieto on voinut joutua kolmannen osapuolen haltuun esimerkiksi asiakirjasta, johon nämä tiedot ovat avain laillisesti ja asiallisesti merkitty. Taustalla voi olla myös tietoturvaloukkaus, jossa ei sinällään ole tapahtunut rikosta, mutta tiedot ovat kuitenkin sen johdosta päätyneet väärinkäyttöjä tekevien käsiin tai esimerkiksi ns. pimeään verkkoon.

Henkilötunnuksen ja muiden yksilöivien tunnistetietojen avulla voi vahinkotarkoituksissa tehdä muuttoilmoituksen tai ilmoittaa henkilön patentti- ja rekisterihallitukselle yhteisön vastuuhenkilöksi kaupparekisteriin, yhdistysrekisteriin tai säätiörekisteriin. Nämä voidaan estää tekemällä muuttosuojaus Digi- ja väestötietovirastoon ja Postiin ja tekemällä rekisteröintikielto patentti- ja rekisterihallitukseen. Muuttoeston voi tehdä Suomi.fi Viestit-palvelun avulla. Palvelu on otettu käyttöön pikaisesti 27.10.2020. Estoja tehtiin muutamissa päivissä jo yli 2000 kappaletta.

Sellaisissa laajamittaisissa tietoturvaloukkauksissa tai tietomurroissa, joissa henkilötietoja on vuotanut tunnistetietojen lisäksi, rikoksen uhrien yksityisyyden loukkaus aiheutuu ennen muuta muista sivullisen tietoon joutuneista tiedoista kuin henkilötunnuksesta. Erityisesti tällainen tilanne on, kun kyseessä on arkaluonteiset potilastiedot. Henkilötunnuksen muuttamisella ei vaikuteta näiden tietojen lainvastaiseen käsittelyyn.

Henkilötunnus harvoin sellaisenaan on jatkorikosten tekovälineenä. Sen avulla on lähinnä mahdollista tehdä petoksia.

Henkilötunnus ei ole viranomaistenkaan rekistereissä salassa pidettävä tieto, mutta sitä koskevat lainsäädännössä määritellyt erityiset käsittelyn edellytykset. Henkilötunnuksen ja muiden yksilöä koskevien tunnistetietojen, kuten nimen ja osoitteen avulla, on rikollisissa tarkoituksissa mahdollista tehdä joissain tilanteissa petoksia. Tämä rajoittuu kuitenkin käytännössä osamaksusopimuksien tekemiseen verkkokaupan yhteydessä ja kulutusluoton hakemiseen sellaisilta toimijoilta, jotka eivät noudata toimialan hyviä käytäntöjä. Luottolaitokset, kuten pankit eivät hyväksy luottahakemuksia ainoastaan henkilön itsensä ilmoittamiin tietoihin perustuen

tekemättä muita tarkistuksia. Identiteettivarkauden kohteeksi joutuneella henkilöllä on myös mahdollisuus tehdä omaehtoinen luottokielto yksityisen palveluntarjoajan rekisteriin, mikä estää luoton myöntämisen.

Mikäli identiteettivarkaus on yksilön tekemän rikosilmoituksen perusteella tai laajamittaisemman tietomurron vuoksi muuten poliisin tutkinnassa tai siitä on annettu tuomio, ei käytännössä asianosaiselle voi aiheutua taloudellista vahinkoa esimerkiksi virheellisesti myönnetyn lainan vuoksi. Myös muut mahdolliset väärällä identiteetillä tehdyt sitoumukset, kuten verkko-ostokset, on tällöin asianosaisen mahdollista toden-taa virheellisiksi eikä näistä aiheudu taloudellisia velvoitteita. Tällaisten asioiden hoitamisesta aiheutuu henkilölle kuitenkin harmia ja haittaa, mikä laajamittaisissa identiteetin väärinkäyttötilanteissa voi olla merkittävääkin.

Henkilötunnuksen muuttamisella voidaan edellä mainittuja väärinkäytöksiä rajoittaa, mutta ei kuitenkaan täysin ehkäistä. Laaja-alaisen tietoturvaloukkauksen tai tietomurron yhteydessä tekijällä tai sillä, joka tällaisen tietovuodon johdosta on saanut käsiinsä henkilötietoja, mukaan lukien henkilötunnuksen, on saamiensa tietojen perusteella mahdollista saada uusikin henkilötunnus tietoonsa, mikäli tämän tiedon onkimiseen on riittävästi taitoa. Kuten edellä on todettu, henkilötunnus ei ole salassa pidettävä tieto, vaan sitä käytetään laajasti yhteiskunnan eri toiminnoissa. Yksilön pitäisi henkilötunnuksen muuttamisen jälkeen olla itse riittävän taitava toimimaan tietoturvallisesti, jottei hänen henkilötunnuksensa joutuisi uudestaan tietovuodon saaneen haltuun.

4.2. Vaikutukset kansalaisille, henkilötunnusta hyödyntäville tahoille ja Digi- ja väestötietovirastolle

Digi- ja väestötietovirasto muuttaa henkilötunnuksen asianosaisen vireille paneman hakemuksen perusteella. Hakemuksen käsittelyn yhteydessä kuullaan henkilöä ja arvioidaan tapausta yksilökohtaisesti. Henkilötunnusta ei voi muuttaa viranomaisaloitteisesti, vaan sen on tapahduttava henkilön aloitteesta. Henkilötunnuksen muuttamisen tarpeellisuuden arvioinnin ja hakemuksen laatimisen tueksi viraston on annettava tarvittavaa informaatiota ja neuvontaa.

Henkilötunnuksen muuttamisella olisi sen haltijalle erilaisia, myös hankaluuksia ja kustannuksia aiheuttavia seurauksia, jotka on yleis- ja tapauskohtaisen neuvonnan keinoin saatettava henkilöiden tietoon ennen mahdollisen henkilötunnuksen muutoshakemuksen vireille panoa. Muun muassa passin, henkilökortin, ajokortin, Kanta palvelun (sis. reseptit), pankkiasiakkuuden uudistaminen sekä siihen liittyvien verkkopankki-tunnusten muuttaminen tulee henkilötunnuksen muuttajan tehtäväksi. Ainoastaan KELA-kortin uusiminen tapahtuu automaattisesti. Lisäksi esimerkiksi koulu- ja työtodistusten osalta henkilön on pyydettävä jokaiselta taholta uusi todistus halutessaan uusilla henkilötiedoillaan.

Digi- ja väestötietovirasto välittää väestötietojärjestelmästä tiedon henkilötunnuksen muuttumisesta eri viranomaisille ja mm. pankeille ja vakuutuslaitoksille, mutta henkilö itse joutuu varmistamaan ja ilmoittamaan henkilötunnuksensa muuttumisesta pienemmille yrityksille, joiden asiakas hän on sekä huolehtimaan muista tarpeellisista jatkotoimista. Käsillä olevassa laajamittaisen ja hyvin julkisen tietomurron tapauksessa on myös huomattava, että henkilö voi joutua tällaisissa asiointitilanteissa yksityiselämänsä suojan kannalta hankalaan asemaan. Henkilötunnuksen muuttaminen on voimassa olevan sääntelyn piirissä harvinaista ja tunnusten aiempaa laajempi muuttaminen saisi todennäköisesti myös laajaa huomiota. Näin henkilö saattaa

tahtomattaan paljastaa arkaluonteisia tietoja tai joutua uteluiden kohteeksi ilmoittaessaan uudesta tunnuksesta tai muuttaessaan asiakirjojaan.

Virasto on arvioinut, että 40 000 henkilötunnuksen muuttamista koskevan hakemuksen käsittely sisältäen diarioinnin, käsittelyn (esittely), päätöksen, tallentamisen ja arkistoinnin, vaatisi virastolta 80 henkilön täysiaikaisen työpanoksen kolmen kuukauden ajan (20 htv). Arvio sisältää myös hakemiseen ja käsittelyyn liittyvän neuvonnan. Keskimääräinen yhden tapauksen kokonaiskäsittelyaika-arvio on 45 minuuttia, kun kaikki edellä mainitut vaiheet lasketaan mukaan. Yhden henkilötyövuoden kustannus on 64.000 euroa ja 20:n henkilötyövuoden 1.280.000 euroa.

Henkilötunnuksen muuttaminen tarkoittaa väestötietojärjestelmässä sitä, että uudesta tunnuksesta tulee järjestelmässä aktiivinen ja vanha tunnus jää historiatiedoksi. Uusi tunnus välitetään pääsääntöisesti väestötietojärjestelmän tietopalvelun yhteydessä eri viranomaisille, esim. rekisterinpäivityksenä tai kyselynä tietojen katselu- tai rajapinta-palvelun kautta.

Digi- väestötietoviraston tietopalveluasiakkaan on mahdollista ja tuleekin päivittää uusi henkilötunnus omaan tietojärjestelmäänsä. Mikäli tietopalveluasiakkaalla on peruste käsitellä myös vanhaa tunnusta historiatietona ja uuteen tunnukseen kytkettynä, se voi näin tehdä, muutoin vanhaa henkilötunnusta koskeva tieto on tuhottava järjestelmästä. Väestötietojärjestelmän tietopalveluista saatavien henkilötunnusmuutosten käsittelyn automaation aste vaihtelee eri tietojärjestelmissä, ja mm. tästä riippuen muutoksesta aiheutuvissa kustannuksissa on toimijakohtaisia eroja. Lisäksi on huomioitava, ettei kaikille yksityisille toimijoille tule automaattisesti uutta henkilötunnusta omiin järjestelmiin tiedon päivittyessä väestötietojärjestelmään. Tämä voi aiheuttaa vaikeuksia toimijoiden asiakkuudenhallinnassa.

4.3. Vaikutukset henkilötunnusjärjestelmään

Mikäli henkilötunnuksen muuttamisesta tehtäisiin nykyisestä helpompaa, voisi sillä ennakoimattomia vaikutuksia koko henkilötunnusjärjestelmän toimivuuteen. Seurauksia voisi aiheutua esim. kaksoisidentiteettien johdosta tapahtuvasta henkilöiden tietojen sekoittumisesta, minkä lisäksi henkilötietojen yhdistäminen eri rekistereiden välillä häiriintyisi. Lainsäädännön keventämisen johdosta aiheutuva henkilötunnusten muutosmäärien kasvu voisi tarkoittaa sitä, että henkilötunnusjärjestelmän nykyinen hyvä toimivuus yhteiskunnan tietohuollon ”linkkinä” merkittävästikin huononisi. Muutos voi aiheuttaa arvaamattomia vaikutuksia henkilötunnuksen käyttämiseen koko yhteiskunnassa, mikäli vaikutuksia ei huolella arvioida.

Tunnusten laajamittainen muuttaminen, mikä voi osoittautua tarpeelliseksi Psykoterapiakeskus Vastaamon tietomurron tapauksessa, aiheuttaa ongelman henkilötunnusten riittävyydelle, erityisesti mikäli uhrien joukossa on maahanmuuttajia sellaisista alkuperämaista, joissa syntymäpäiväksi virallisiin rekistereihin ja dokumentteihin merkitään usein 1. tammikuuta henkilön todellisesta syntymäpäivästä riippumatta.

Jo nyt tiettyjen vuosien 1. tammikuuta syntymäpäivillä on käytössä enää joitain kymmeniä vapaita tunnuksia. Henkilötunnuksen uudistamisen valmistelun yhteydessä on arvioitu, että nykyisillä menettelyillä tunnukset tietyiltä kriittisiltä päiviltä voivat loppua jo 2-3 vuoden päästä. Tämä arvio perustuu siihen, että noin 30 uutta tunnusta myönnetään yhdelle syntymäpäivälle vuosittain. Yksittäinen laajamittainenkaan tunnusten muuttamisaalto ei kerralla todennäköisesti aiheuttaisi tunnusten loppumista, mutta se voisi siinä määrin merkittävästi lisätä yksittäiselle päivälle

annettavia tunnuksia, että riittävyyden varmistamisen ratkaisu tulee olla käyttöönotettavissa jo vuoden 2022 alussa.

Lainsäädännössä ei ole varauduttu siihen, miten toimittaisiin tilanteessa, että vapaat henkilötunnukset loppuvat jonkin syntymäpäivämäärän osalta, Myös tätä koskevan säätelyn aikaansaamista voidaan pitää entistä kriittisempänä asiana, mikäli henkilötunnuksen muuttamisen perusteluja kevennetään.

Henkilötunnuksen uudistamisen työryhmän jatkotyön virkamiesvalmistelussa on ehdotettu, että riittävyyden varmistamiseksi henkilötunnuksessa otettaisiin käyttöön uusia välimerkkejä. Uuden välimerkin käyttöönottaminen organisaatioiden tietojärjestelmissä edellyttää järjestelmämuutoksia, joiden avulla järjestelmät voivat käsitellä uuden välimerkin mukaisia identiteettejä ja niihin liittyviä tietoja. Tämän muutoksen käyttöönottaminen yhteiskunnassa edellyttää arvion mukaan vähintään kahden vuoden siirtymäaikaa. Uuden välimerkin käyttöönottamisen vaikutusten arviointi on käynnistymässä.

5. Muut toteuttamisvaihtoehdot ja kehityshankkeet

Henkilötunnuksen uudistamista selvittänyt työryhmä on loppuraportissaan todennut, että henkilötunnuksen uudistamisen tavoiteltavia hyötyjä ei täysimääräisesti saavuteta, jos nykyisen kaltainen henkilötunnusten hallitsematon käyttö henkilön tunnistamisessa ei muutu. Yksinomaan henkilötunnuksella ei tulisi olla mahdollista tunnistaa eli varmentaa sitä, onko fyysisesti asioiva henkilö todella se henkilö, joka väittää olevansa. Henkilön yksilöivän tunnisteen muoto ei myöskään ratkaise tunnistamiskäytäntöihin liittyviä riskejä, ellei säännellä lisäksi sen käytöstä henkilön tunnistamiseen asioinnissa.

Henkilötunnuksen uudistamista selvittänyt työryhmä on ehdottanut, että jatkotyössä olisi tarkasteltava, voitaisiinko henkilötunnuksen käyttöä henkilön tunnistuksessa lainsäädännön keinoin jotenkin ohjata tai rajoittaa sekä mahdollisesti säätää tarkemmin, jotta henkilötunnusta käytettäisiin jatkossa ainoastaan tunnisteena, joka olisi avain tietojärjestelmien välillä henkilöiden yksilöintiin ja erotteluun. Myös henkilötunnuksen julkisuutta tulisi arvioida siitä näkökulmasta, miten tämän tiedon mahdollinen julkisuus vaikuttaisi ei toivottuun käytäntöön käyttää henkilötunnusta yhtenä tunnistautumiskeinona. Henkilö tulisi tunnistaa sähköisellä välineellä tai varmistaa yksilöivillä ominaisuuksilla riittävän vahvasti. Henkilön yksilöinnin tavoitetilalla onkin kiinteä yhteys sähköisen tunnistamisen kehittymiseen Suomessa. Käyntiasioinnissa henkilöllisyyden osoittaminen tulisi mahdollistaa henkilöllisyysasiakirjan lisäksi myös sähköisellä tunnistautumisella. Henkilön tunnistamisen vaatimuksia tulee jatkotyössä arvioida erityisesti suhteessa hallintolakiin, lakiin sähköisestä asioinnista viranomaistoiminnassa (13/2003) sekä lakiin digitaalisten palvelujen tarjoamisesta (306/2019).

Henkilötunnuksen uudistamisen selvittänyt työryhmä ei tehnyt konkreettisia sääntelyn muutosehdotuksia.

Seuraavissa kappaleissa kuvatut toimenpiteet kytkeytyvät henkilöiden identiteetin hallintaan ja digitaalisen toimintaympäristön toimintamalleihin yhteiskunnassa. Ehdotetuista toimenpiteistä osa on välittömiä, lyhyellä aikavälillä toteutettavia toimenpiteitä, osa rakenteellisia pitempää valmistelua edellyttäviä toimia. Toimien tavoitteena on auttaa tietomurron uhreja akuutissa tilanteessa ja edistää henkilötunnuksen kestäviä käyttötapoja yhteiskunnassa siten, että

henkilötunnusta käsitellään yksilöintitietona, ei tunnistuskeinona. Tavoitteena on myös vähentää henkilötunnuksella tehtävien väärinkäytösten mahdollisuuksia ja vähentää tietoturvaloukkausten ja tieto- ja viestintärikosten uhreiksi joutuneille aiheutuvaa vahinkoa vääriin käsiin joutuneista identiteettitiedoista.

5.1. Lyhyen aikavälin toimenpiteet

5.1.1. Henkilötunnuksen käsittelyä koskevien käytäntöjen ohjaus

Henkilötunnuksen uudistamistyö on ollut käynnissä viime vaalikaudella asetetun valtiovarainministeriön työryhmän puitteissa vuodesta 2017 alkaen. Henkilötunnuksen ympärille rakentuvaa identiteetinhallintaa on uudistettava useastakin syystä yhteiskunnassa. Henkilötunnusten riittävyys on varmistettava, organisaatioiden antamista keinotekoisista henkilötunnuksista on luovuttava yhtenäisen tunnusjärjestelmän kattavuuden varmistamiseksi, Suomeen tuleville henkilöille on saatava nykyistä sujuvammin ja nopeammin henkilötunnus asiointimahdollisuuksien varmistamiseksi. Henkilötunnuksen uudistamisen yhteydessä on tullut esiin myös ongelmat henkilötunnuksen käsittelytavoissa. Näitä voidaan parhaiten ja koko henkilötunnusjärjestelmän nykyiset ja tulevat tarpeet varmistaen edistää tämän uudistuksen yhteydessä. Ottaen huomioon nykyisen henkilötunnusjärjestelmän keskeinen asema koko yhteiskunnassa, tulee järjestelmään tehtävät muutokset arvioida kattavasti ja huolellisesti jo pelkästään riskienhallinnan näkökulmasta.

Henkilötunnuksen käyttöä koskevia edistämistoimia, kuten kansalaisten informoimista ja hyvien käytäntöjen ohjaamista voidaan toteuttaa lyhyellä aikavälillä vuoden 2020 loppuun mennessä asetettavassa henkilötunnuksen uudistamishankkeessa. Erityisesti koottu ja eri viranomaisten ja toimijoiden näkökulmat esiin tuova yhtenäinen kansalaisviestintä voi auttaa myös Vastaamon tietomurtotapauksen asianosaisia huolehtimaan omien identiteettitietojensa mahdollisimman hyvästä turvaamisesta. Tätä tietoa on jo saatavilla muun muassa tietovuotoapu.fi –sivustolta, Digi- ja väestötietoviraston suomi.fi/fi/tietomurto -sivustolta, Patentti- ja rekisterihallituksesta ja tietosuojavaltuutetun toimiston nettisivuilta. Myös media on jo monilla tavoin tarjonnut ajantasaista tietoa.

Henkilötunnuksen uudistustoiminpiteiden tarkoituksena on myös kokonaisuutena edistää henkilötunnuksen käyttöä nimenomaan yksilöintitarkoituksessa ja parantaa identiteetinhallinnan järjestelmää digitalisoituvassa yhteiskunnassa. Se edellyttää sekä henkilötunnuksen hallintamenettelyjen kehittämistä että myös samanaikaisesti totutuista henkilötunnuksen käsittelytavoista luopumista. Tähän kytkeytyy myös tunnistamiseen ja pääsynhallintaan liittyvien menettelyjen parantaminen sekä lokitietojen kerääminen asiointitapahtumista, jotta mahdolliset väärinkäytökset voidaan ehkäistä ja jäljittää paremmin. Näihin tähtääviä toimenpiteitä voidaan tehdä pidemmällä aikavälillä.

Henkilötunnuksen käsittelyä koskevien käytäntöjen ohjaukseen liittyviin toimenpiteisiin osallistuisivat useat viranomaiset ja yhteistyöhön ja parempien käytäntöjen toteuttamiseen kutsuttaisiin laajasti myös muita yhteiskunnan toimijoita kuten järjestöjä ja elinkeinoelämän toimijoita. Toimenpiteet valmisteltaisiin valtiovarainministeriön johdolla.

Tietosuojavaltuutettu on käynnistänyt arvion, voiko nykyistä henkilötunnuksen käsittelyä koskevaa linjaa tiukentaa. Arvion kohteena on erityisesti hyödykesidonnaisten kertaluottojen ja laskutuspalvelujen tarjoaminen, joita ei koske säädösperusteisesti henkilön tunnistamista koskevia vaatimuksia.

5.1.2. Henkilötietojen sulku- ja estopalvelujen kokoaminen

Identiteettivarkauden johdosta eri henkilöillä voi olla erilaisia tarpeita hakea estoja ja kieltoja. Estoja ja kieltoja koskeva lainsäädäntö on hajautunut. Estojen ja kieltojen hakemiseen voi myös liittyä viranomaisen harkintaa. Osaa estoista ja kielloista ylläpitävät myös yksityiset tahot ja ne voivat olla maksullisia palveluja.

Lyhyellä aikavälillä on toteutettu erilaisten tietojen käsittelyä koskevien kielto- ja estopalvelujen kokoaminen yhteen paikkaan. Tiedot ja linkit on saatavilla sivustolla suomi.fi/fi/tietomurto. Tämä helpottaa identiteettivarkauksien uhrien tilannetta.

Lisäksi lyhyellä aikavälillä on myös selvitettävissä, voitaisiinko tällaiset kiellot hakea ja aktivoida yhden viranomaispalvelun kautta, joko suoraan yhdestä palvelusta tai kertakirjautumisen kautta useiden toimijoiden palveluista, ja minkälaisia mahdollisia säädösmuutoksia tämä edellyttäisi. Mikäli näissä toiminnallisuuksissa halutaan edetä toteutukseen, on kustannukset, aikataulut ja vaikutukset viranomaisten toimintaan arvioitava osana jatkovalmistelua

Tämän tavoitteen täysimääräinen toteutuminen edellyttää myös sitä, että nekin (esim. yksityiset tahot), joilla ei ole Suomi.fi -palvelujen käyttövelvollisuutta, olisivat halukkaita ylläpitämään tietojaan palvelutietovarannossa ja mahdollisesti myös tuomaan asiakkaiden tietoja asiakkaan henkilökohtaiseen palvelunäkymään.

Yhtenä alustavan mahdollisuutena on nähty, että nykyiset jo tehdyt sisällöt tietovuodon uhrille ja Suomi.fi -palvelutietovarannossa olevat palvelut ja palvelukanavat voisi rakentaa uudelleen opastavan polun muotoon. Opastavan polun toteuttaminen vaatisi niin sisältötyötä (verkkotoimitus) kuin palvelu- ja sisältömuotoilua ja teknistä toteutusta, testausta ja käännöksiä. Työ olisi mahdollista käynnistää pikaisesti suunnittelun osalta, mikäli tähän olisi rahoitusta saatavilla.

5.2. Pidemmän aikavälin toimenpiteet

5.2.1. Digitaalinen henkilöllisyys ja tunnistaminen

Kuten edellä tullut esille, henkilötunnuksen ja muiden henkilöä yksilöivien tietojen käyttäminen tunnistamisen keinona on ongelma. Nykytilanteeseen on vaikuttanut osaltaan se, että henkilötunnukseen tietona luotetaan yleisesti ja sen kysyminen asiointitilanteessa on vaivatonta. Toisaalta samaan aikaan tietoturvallisten tunnistamismenetelmien käyttöön liittyy haasteita. Yhtenä haasteena luotettavien ja tietoturvallisten tunnistamiskeinojen edistämisessä on se, että tunnistusvälineet eivät ole yhdenvertaisesti kaikkien suomalaisissa palveluissa asioivien henkilöiden saatavilla. Lisäksi haasteena on se, etteivät kaikki toimijat ole valmiita käyttämään palveluissaan vahvan sähköisen tunnistamisen menettelyjä. Tähän voi liittyä yhtäältä arviot vahvan sähköisen tunnistamismenettelyjen soveltuvuudesta palveluntarjoajan muuhun palvelukokonaisuuteen tai mahdollisesti nykyisten tunnistuspalvelujen hinta.

Jo käynnissä olevana toimenpiteenä voidaan jatkaa valtiovarainministeriön Digitaalisen henkilöllisyyden hanketta, jossa kehitetään toimintamalli ja tuotetaan tarvittavat ratkaisut, joiden avulla valtion takaama digitaalinen henkilöllisyys voidaan tarjota digitaalisena henkilöllisyystodistuksena henkilöiden käyttöön. Tämä edistää osaltaan yhä laajemmin ottamaan käyttöön tietoturvallisia tapoja henkilöllisyyden todentamiseen. Digitaalisen henkilöllisyyden hankkeen on tarkoitus päättyä vuonna 2022.

5.2.2. Digitaalinen turvallisuuden periaatepäätöksen toimeenpano

Keväällä 2020 valtioneuvoston hyväksymässä julkisen hallinnon digitaalisen turvallisuuden periaatepäätöksessä määritetään kehittämisen periaatteet ja keskeiset palvelut turvallisuuden edistämiseksi digitaalisessa toimintaympäristössä. Tavoitteena on kokonaisturvallisuuden viitekehyksessä suojata kansalaisia, yhteisöjä ja yhteiskuntaa niiltä riskeiltä ja uhkilta, jotka voivat kohdistua tietoihin, palveluihin ja yhteiskunnan toimintaan digitaalisessa toimintaympäristössä. Kansalaisten, yritysten ja yhteisöjen tulee voida luottaa eettisesti kestäviin, avointa ja läpinäkyvää toimintaa tukeviin ja turvallisiin julkisen hallinnon palveluihin. Digitalisoitumiseen sekä digitaalisen toiminnan ja palveluiden turvaamiseen on siten panostettava tasapainoisesti.

Digitaalisen turvallisuuden kehittämisen koordinaatiota ja yhteistyötä sekä taloudellisen vaikuttavuuden arviointia vahvistetaan. Kansalaisten ja henkilöstön osaamista sekä palveluiden turvallisuutta edistetään. Tämä tukee kyberturvallisuusstrategian 2019 toteuttamista julkisessa hallinnossa.

Digitaalisen turvallisuuden periaatepäätöksen toimenpanemiseksi on asetettu valtioneuvoston yhteinen Haukka-ohjelma.

5.2.3. Henkilöllisyyden todentamisen toimintamallien ja lainsäädännön kehittämistarpeiden selvittäminen

Henkilön identiteetin hallinnan ja siten samalla henkilön yksilöivien tietojen käsittelyn kannalta keskeinen kehityksen ja mahdollisten toimintamallien kehittämisen ja lainsäädäntötoimenpiteiden kohde on erilaisissa asiointitilanteissa toteutettavat menettelytavat henkilöllisyyden todentamiseksi. Velvoittavaa sääntelyä henkilöllisyyden todentamiseen tulisi arvioida erityisesti, jos asioinnissa on mahdollisuus tehdä merkittäviä oikeustoimia. Henkilöllisyyden todentamisvelvollisuuden laajentaminen sellaisiin oikeustoimiin ja aloille, joille laissa ei nykyisin tällaista velvoitetta aseteta, olisi syytä huolellisesti arvioida. Tämä koskee sekä viranomais- että yksityisen sektorin toimintaa.

Muutoksilla on vaikutuksia kuluttajien ja yritysten mahdollisuuksiin tehdä sopimuksia verkossa, joten niitä tulisi arvioida huolellisesti. Viranomaisten käytäntöjen osalta olisi huomioitava myös vaikutukset perustuslain turvaamaan yhdenvertaisuuteen ja muut perusoikeusvaikutukset. Todentamisvelvollisuuden laajentaminen olisi arvioitava myös luottamusyhteiskunnan perusteita vasten, esimerkiksi sen suhteen, että hyväksymmekö jatkossa sen, että kaikilla on oltava joko fyysinen tai mobiilihenkilötunnus asiointia varten ja mahdollisesti vielä niin, että se on luotettavan asioinnin varmistamiseksi oltava aina mukana.

Tämän linjausehdotuksen yhteydessä ei ole arvioitu esimerkiksi tietoturvallisuuden parantamisen yleisiä toimenpiteitä.

5.2.4. Kuluttajasuojalaki

Henkilötunnuksen ja muiden yksilöä koskevien tunnistetietojen, kuten nimen ja osoitteen avulla, on rikollisissa tarkoituksissa mahdollista tehdä joissain tilanteissa petoksia. Esimerkiksi kuluttajakaupassa edellytetään kuitenkin jo voimassa olevan lainsäädännön nojalla laajalti vahvaa tunnistamista haettaessa luottoa tai maksettaessa ostos verkossa. Velvollisuus todentaa kuluttajansuojalain mukaisesti luottoa hakevan henkilön henkilöllisyys huolellisesti koskee niin luottolaitoksia kuin muita elinkeinonharjoittajia, jotka myöntävät kuluttajille luottoja, eli myös ns. pikaluottoyrityksiä. Kilpailu- ja kuluttajavirastosta saatujen tietojen mukaan myöskään näiden säännösten noudattamisessa ei ole ilmennyt merkillepantavia ongelmia.

Kuluttajansuojalain säännökset henkilöllisyyden todentamisesta eivät koske hyödykesidonnaisia kertaluottoja tai laskutuspalveluja, joita tarjotaan monesti yhtenä rahoitusvaihtoehtona verkossa ostoksia maksettaessa. Kun henkilöllisyyden todentamista koskevat säännökset lisättiin kuluttajansuojalakiin vuonna 2009, tiedossa olivat lähinnä ns. pikaluottoihin liittyvät ongelmat.

EU-direktiiviin pohjautuvassa maksupalvelulaissa 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.

Keväällä 2021 käynnistettävän kuluttajaluottosäännösten uudistamista koskevan hankkeen yhteydessä arvioidaan, tuleeko kuluttajansuojalain 7 luvun lainanhakijan henkilöllisyyden todentamisesta sääntelyä tiukentaa laajentamalla se koskemaan kaikkien kuluttajaluottosopimusten tekemistä. Lainsäädäntöesitys arvioidaan voitavan antaa syksyllä 2021.