SISÄASIAINMINISTERIÖ

Henkilöllisyyden luomista koskeva hanke

(identiteettiohjelma)

Työryhmän loppuraportti

Sisäinen turvallisuus

SISÄASIAINMINISTERIÖN JULKAISUJA 32/2010

SISÄASIAINMINISTERIÖ
Sisäinen turvallisuus

Henkilöllisyyden luomista koskeva hanke

(identiteettiohjelma)

Työryhmän loppuraportti

Helsinki 2010

Sisäasiainministeriö
Helsinki
Helsinki 2010

ISSN 1236-2840
ISBN 978-952-491-619-6 (nid.)
ISBN 978-952-491-620-2 (PDF)

SISÄASIAINMINISTERIÖ

KUVAILULEHTI
15.12.2010

Tekijät (toimielimestä, toimielimen nimi, puheenjohtaja, sihteeri)	Julkaisun laji
Neuvotteleva virkamies Johanna Kari, puheenjohtaja	Työryhmämuistio
	Toimeksiantaja Sisäasiainministeriö
	Toimielimen asettamispäivä 29.10.2008, SM092:00/2008

Julkaisun nimi
Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma), ryhmän loppuraportti

Julkaisun osat
muistio

Tiivistelmä

Sisäasiainministeriö asetti 29.10.2008 hankkeen valtion vahvistaman henkilöllisyyden luomista koskevien menettelytapojen sekä henkilöllisyyttä koskevan lainsäädännön laatimiseksi. Hankkeen tavoitteena oli laatia kattava identiteettiohjelma, jossa kuvataan henkilöllisyyden luomiseen liittyvä nykytila, kehitysnäkymät ja riskit sekä tuodaan esille johtopäätökset ja toimenpidesuositukset. Identiteettiohjelma on samalla kokonaisvaltainen suunnitelma, jolla valtio tulevaisuudessakin suojaa kansalaisten henkilöllisyyttä sekä perinteisessä että sähköisessä toimintaympäristössä. Työryhmän toimikausi oli 29.10.2008 - 15.12.2010.

Työryhmän keskeiset johtopäätökset ja toimenpidesuositukset ovat seuraavat:

- Ajokortin käytön uudelleentarkastelu tunnistamisasiakirjana
- Passin ja henkilökortin yhteismyöntöprosessin selvittäminen
- Sulkulistapalvelun selvittäminen ajokorttien, henkilökorttien ja passien osalta
- Tunnistamisen merkityksen korostaminen ja tietoisuuden lisääminen
- Identiteettivarkaudet:

  1. Toisena esiintyminen rajoittaa henkilön tiedollista itsemääräämisoikeutta
  2. Uhrin heikko asema rikosprosessissa
  3. Keskitetty ilmoitusjärjestelmä identiteettivarkauden uhrille
  4. Identiteettiturvallisuuden neuvottelukunta
  5. Toimintaohje identiteettivarkauden uhrille
  6. Jatkotyöryhmän perustaminen, jossa tarkastellaan oikeusministeriön johdolla identiteettivarkauksia koskevan lainsäädännön todellinen vaikuttavuus ja tehdään tiedon keräämistä koskevien tunnusmerkistöjen ja toimivaltuuksien lähempi jatkotarkastelu

- Biometristen tunnistusratkaisujen säädöstarve on ilmeinen
- Turvapaikanhakijan asiointikortin käyttöönoton selvittäminen
- Sisäasiainministeriön poliisiosasto ja Poliisihallitus lisäksi ehdottavat: Selvitystä henkilöllisyyttä osoittavia asiakirjoja koskevan lainsäädännön tarpeellisuudesta sekä henkilökorttilain muutosta (biometriset tunnisteet)

Avainsanat (asiasanat)
henkilöllisyys, ajokortit, henkilökortit

Muut tiedot
Sähköisen julkaisun ISBN 978-952-491-620-2 (PDF), osoite www.intermin.fi/julkaisut

Sarjan nimi ja numero		ISSN	ISBN
Sisäasiainministeriön julkaisut 32/2010		1236-2840	978-952-491-619-6
Kokonaissivumäärä 116	Kieli suomi	Hinta 25 € + alv	Luottamuksellisuus julkinen
Jakaja Sisäasiainministeriö		Kustantaja/julkaisija Sisäasiainministeriö	

INRIKESMINISTERIET

PRESENTATIONSBLAD
15.12.2010

Författare (uppgifter om organet: organets namn, ordförande, sekreterare)	Typ av publikation
Konsultativ tjänsteman Johanna Kari, ordförande	Promemoria av arbetsgruppen
	Uppdragsgivare: Inrikesministeriet
	Datum för tillsättandet av organet: 29.10.2008, SM092:00/2008

Publikation (även den finska titeln)
Projekt rörande skapande av identitet (identitetsprogrammet), arbetsgruppens slutrapport

Publikationens delar
Promemoria

Referat

Den 29 oktober 2008 tillsatte inrikesministeriet ett projekt med uppgift att definiera tillvägagångssätt för skapande av statligt bestyrkt identitet och utarbeta lagstiftning om identitet. Målet var ett omfattande identitetsprogram som beskriver nuläget, utvecklingsutsikterna och riskerna när det gäller skapande av identitet och som presenterar slutsatser och rekommendationer. Identitetsprogrammet var samtidigt avsett som en heltäckande plan genom vilken staten framöver ska skydda medborgarnas identitet i både elektroniska och icke-elektroniska sammanhang. Arbetsgruppens mandatperiod började den 29 oktober 2008 och slutade den 15 december 2010.

Arbetsgruppen presenterar följande centrala slutsatser och rekommendationer:

- Användningen av körkort som legitimationshandling bör ses över.
- Samutfärdande av pass och identitetskort bör utredas.
- Spärrlistans funktion bör utredas när det gäller körkort, identitetskort och pass.
- Vikten av identifiering bör betonas och medvetenheten i frågan ökas.
- Identitetsstölder:

1. Självbestämmanderätten över egen information inskränks när en person uppträder som någon annan.
2. Offrets ställning i brottsmålsprocessen är svag.
3. Offer av identitetsstöld behöver ett centralt anmälningssystem.
4. Delegation för identitetssäkerhet
5. Anvisningar om hur man ska gå till väga när man har råkat ut för identitetsstöld
6. En fortsättande arbetsgrupp under ledning av justitieministeriet bör tillsättas med uppgift att följa med vilken påverkan lagstiftningen om identitetsstöld har och göra en fördjupad granskning av definitionerna och befogenheterna för insamling av information.

- Behovet av lagstiftning som reglerar biometriska identifikationslösningar är uppenbart.
- Införande av ett tillfälligt kort för asylsökande bör utredas.
- Inrikesministeriets polisavdelning och Polisstyrelsen föreslår därtill en utredning om behovet av lagstiftning om identitetshandlingar och en revidering av lagen om identitetskort (biometriska kännetecken).

Nyckelord
identitet, körkort, identitetskort

Övriga uppgifter
Elektronisk version, ISBN 978-952-491-620-2 (PDF), www.intermin.fi/publikationer

Seriens namn och nummer		ISSN	ISBN
Inrikesministeriets publikation 32/2010		1236-2840	978-952-491-619-6
Sidoantal	**Språk**	**Pris**	**Sekretessgrad**
116	finska	25 € + moms	offentlig
Distribution		**Förläggare/utgivare**	
Inrikesministeriet		Inrikesministeriet	

Sisäasiainministeriölle

Sisäasiainministeriö asetti 29.10.2008 hankkeen valtion vahvistaman henkilöllisyyden luomista koskevien menettelytapojen sekä henkilöllisyyttä koskevan lainsäädännön laatimiseksi. Hankkeen tavoitteena oli laatia kansallinen identiteettiohjelma, joka sisältää kokonaisvaltaisen suunnitelman valtion tehtävistä henkilöllisyyden luomisessa yhteiskunnassa sekä keinoista, joilla valtio tulevaisuudessakin suojaa kansalaisten henkilöllisyyden sekä perinteisessä että sähköisessä toimintaympäristössä.

Eräänä erityisenä painopistealueena olivat identiteettivarkaudet ja niiden ennalta ehkäisy. Hankkeessa määritellään ne asiakirjat, joilla henkilöllisyys voidaan luotettavasti todentaa sekä määritellään tunnistamisprosessien luotettavuus. Myös ulkomaalaisten varmistamatonta henkilöllisyyttä koskevat erityiskysymykset otettiin huomioon.

Identiteettiohjelman keskeisiä tavoitteita oli määritellä ja kartoittaa:

- Henkilöllisyyden määrittely
- Henkilöllisyyden suojaaminen
- Valtion tehtävä henkilöllisyyksien luojana sekä vastuuviranomaiset
- Identiteettivarkauksien ennalta estäminen sekä kriminalisoinnin tarpeen selvittäminen.
- Tunnistaminen ja siinä käytettävät tunnistamisasiakirjat
- Biometriikan käyttömahdollisuudet ja toteuttamistavat tunnistamisasiakirjojen osalta

Identiteettivarkauksien kriminalisoinnin tarpeen selvittäminen on lisätty työryhmän toimeksiantoon asettamiskirjeen jälkeen. Valmisteltaessa Valtioneuvoston periaatepäätöstä sähköisestä tunnistamisesta (5.3.2009), ovat oikeusministeriö, valtiovarainministeriö, liikenne- ja viestintäministeriö ja sisäasiainministeriö sopineet, että sisäasianministeriö tekee identiteettivarkauksien kriminalisoinnin esiselvitysvaiheen Henkilöllisyyden luomista koskevassa hankkeessa (identiteettiohjelma).

Hanketyöryhmään ovat kuuluneet:
Neuvotteleva virkamies Johanna Kari, sisäasiainministeriön poliisiosasto (puheenjohtaja), tietohallintojohtaja Kaarlo Korvola sisäasiainministeriö, ylitarkastaja Tiina Nuutinen sisäasiainministeriön poliisiosasto, poliisitarkastaja Joni Länsivuori sisäasiainministeriön poliisiosasto, erityisasiantuntija Olli-Pekka Rissanen valtiovarainministeriö, rekisteröintipäällikkö Tuire Saaripuu Väestörekisterikeskus (sijainen rekisteröintipäällikkö Katja Häkkinen), kehityspäällikkö Jan Partanen Väestörekisterikeskus, lainsäädäntöneuvos Kirsi Miettinen liikenne- ja viestintäministeriö, ylitarkastaja Heikki Huhtiniemi tietosuojavaltuutetun toimisto, ylitarkastaja Elina Immonen sisäasiainministeriön maahanmuutto-osasto, ylitarkastaja Wivi-Ann Wagello-Sjölund sisäasiainministeriön maahanmuutto-osasto (30.7.2010 saakka), yksikön päällikkö Hilkka Nenonen ulkoasiainmi-

nisteriö (1.8.2009 alkaen maahantuloasioiden koordinaattori Seija Haarala), tiimin vetäjä Jaana Honkakunnas ulkoasiainministeriö, projektipäällikkö Ismo Parviainen Poliisihallitus, poliisitarkastaja Timo Laine Poliisihallitus, ylitarkastaja Kimmo Pylväs Poliisihallitus, ylitarkastaja Jukka Hertell Poliisihallitus, ylitarkastaja Sari Kajantie, Keskusrikospoliisi, tutkija Kari Kanto Keskusrikospoliisi sekä ylikonstaapeli Marko Forss Helsingin poliisilaitos. Työryhmän teknisenä sihteerinä on toiminut osastosihteeri Sini Kallonen sisäasiainministeriön poliisiosastolta.

Ulkomaalaisasioita on käsitelty erillisissä ulkomaalaisteemakokouksissa, joihin on kutsuttu ulkomaalaisasioiden asiantuntijoita. Näissä kokouksissa on myös valmisteltu raportin ulkomaalaisia koskevat osiot. Biometriaa koskevat osiot on tehty pääosin edellisen sisäasiainministeriön poliisiosaston biometriahankkeen toimesta.

Työryhmän työhön ovat osallistuneet asiantuntijoina seuraavat henkilöt: lupahallintopäällikkö Minna Gråsten Poliisihallitus, neuvotteleva virkamies Tiina Ferm sisäasiainministeriö, lakimies Gunveig Planting-Visa Kuluttajavirasto, ylitarkastaja Heikki Partanen tietosuojavaltuutetun toimisto, tulosalueen johtaja Hanna Helinko Maahanmuuttovirasto, ylitarkastaja Raisa Bernards Maahanmuuttovirasto, ylitarkastaja Marjo Mäkelä Maahanmuuttovirasto, hankejohtaja Hilkka Vanhatalo Maahanmuuttovirasto, tulosalueen johtaja Ulla Vainikka Maahanmuuttovirasto, ylitarkastaja Pia Salmela sisäasiainministeriön maahanmuutto-osasto, komisario Arvo Mäntykenttä Helsingin poliisilaitos, ylitarkastaja Jukka Tukia Maahanmuuttovirasto, teknologiapäällikkö Olli Lehtoranta hallinnon tietotekniikkakeskus, toimistosihteeri Elina Lappalainen ulkoasiainministeriö, kehityspäällikkö Kaj Välimäki Väestörekisterikeskus, lainsäädäntöneuvos Johanna Puiro sisäasiainministeriö, rikoskemisti Vuokko Ljungberg keskusrikospoliisi sekä rikosinsinööri Petri Varjos keskusrikospoliisi.

Poliisin hallintorakenneuudistuksessa on 1.1.2010 perustettu uusi virasto Poliisihallitus. Sisäasiainministeriön poliisiosasto on myös organisoitu uudelleen. Suurin osa hankkeen työstä on tehty edellisen SM/PO:n aikana ennen vuotta 2010. Suuri osa edellisen SM/PO:n henkilöstöstä on siirtynyt uudistuksessa Poliisihallituksen palvelukseen. Poliisihallituksesta on nimetty uudet jäsenet työryhmään.

Työryhmä on toiminut ajalla 28.10.2008 - 15.12.2010.

Työryhmä on kokoontunut 20 kertaa, joista 2 on ollut ulkomaalaisteemakokouksia. Työ on tehty virkatyönä. Hanke on teettänyt asettamiskirjeen mukaisesti riskianalyysin tunnistamisprosessiin liittyvistä riskeistä koskien passeja, henkilökortteja ja kansalaisvarmennetta. Esille tulleista riskeistä kerrotaan enemmän kohdassa 4.2.1.

Loppuraporttiluonnoksesta on ennen työn valmistumista pyydetty lausunnot hanketyöryhmän lisäksi seuraavilta tahoilta: oikeusministeriö, vähemmistövaltuutetun toimisto, Maahanmuuttovirasto, Helsingin maistraatti, Finanssialan keskusliitto sekä Finanssivalvonta. Annetut lausunnot on huomioitu lopullisessa raportin tekstissä.

Työryhmän keskeiset johtopäätökset ja toimenpidesuositukset ovat seuraavat:

- Ajokortin käytön uudelleentarkastelu tunnistamisasiakirjana
- Passin ja henkilökortin yhteismyöntöprosessin selvittäminen
- Sulkulistapalvelun selvittäminen ajokorttien, henkilökorttien ja passien osalta
- Tunnistamisen merkityksen korostaminen ja tietoisuuden lisääminen
- Identiteettivarkaudet:
  1. Toisena esiintyminen rajoittaa henkilön tiedollista itsemääräämisoikeutta
  2. Uhrin heikko asema rikosprosessissa
  3. Keskitetty ilmoitusjärjestelmä identiteettivarkauden uhrille
  4. Identiteettiturvallisuuden neuvottelukunta
  5. Toimintaohje identiteettivarkauden uhrille
  6. Jatkotyöryhmän perustaminen, jossa tarkastellaan oikeusministeriön johdolla identiteettivarkauksia koskevan lainsäädännön todellinen vaikuttavuus ja tehdään tiedon keräämistä koskevien tunnusmerkistöjen ja toimivaltuuksien lähempi jatkotarkastelu
- Biometristen tunnistusratkaisujen säädöstarve on ilmeinen
- Turvapaikanhakijan asiointikortin käyttöönoton selvittäminen
- SM/PO ja Poliisihallitus lisäksi ehdottavat: Selvitystä henkilöllisyyttä osoittavia asiakirjoja koskevan lainsäädännön tarpeellisuudesta sekä henkilökorttilain muutosta (biometriset tunnisteet)

Raportin liitteenä on ulkoasiainministeriön kokoama taulukko EU-maiden henkilökorteista (liite 1).

Lisäksi liitteenä on liikenne- ja viestintäministeriö raportista jättämä lausuma.

Työryhmän loppuraportti sisäasiainministeriölle

Helsingissä 15. joulukuuta 2010

Johanna Kari

Korvola Kaarlo

Olli-Pekka Rissanen

Kirsi Miettinen

Tiina Nuutinen

Joni Länsivuori

Elina Immonen

Seija Haarala

Heikki Huhtiniemi

Jan Partanen

Jaana Honkakunnas

Katja Häkkinen

Timo Laine

Sari Kajantie

Kari Kanto

Kimmo Pylväs

Marko Forss

Ismo Parviainen

Sini Kallonen

Sisällys

Liitteet

1 Työryhmän asettaminen ja tehtävät

Sisäasiainministeriö asetti 29.10.2008 hankkeen valtion vahvistaman henkilöllisyyden luomista koskevien menettelytapojen sekä henkilöllisyyttä koskevan lainsäädännön laatimiseksi. Hankkeen tavoitteena on laatia kansallinen identiteettiohjelma, joka sisältää kokonaisvaltaisen suunnitelman valtion tehtävistä henkilöllisyyden luomisessa yhteiskunnassa sekä keinoista, joilla valtio tulevaisuudessakin suojaa kansalaisten henkilöllisyyden sekä perinteisessä että sähköisessä toimintaympäristössä. Työryhmän toimikausi oli 29.10.2008 - 15.12.2010.

Hanketyöryhmään ovat kuuluneet:
Neuvotteleva virkamies Johanna Kari, sisäasiainministeriön poliisiosasto (puheenjohtaja), tietohallintojohtaja Kaarlo Korvola sisäasiainministeriö, ylitarkastaja Tiina Nuutinen sisäasiainministeriön poliisiosasto, poliisitarkastaja Joni Länsivuori sisäasiainministeriön poliisiosasto, erityisasiantuntija Olli-Pekka Rissanen valtiovarainministeriö, rekisteröintipäällikkö Tuire Saaripuu Väestörekisterikeskus (sijainen rekisteröintipäällikkö Katja Häkkinen), kehityspäällikkö Jan Partanen Väestörekisterikeskus, lainsäädäntöneuvos Kirsi Miettinen liikenne- ja viestintäministeriö, ylitarkastaja Heikki Huhtiniemi tietosuojavaltuutetun toimisto, ylitarkastaja Elina Immonen sisäasiainministeriön maahanmuutto-osasto, ylitarkastaja Wivi-Ann Wagello-Sjölund sisäasiainministeriön maahanmuutto-osasto (30.7.2010 saakka), yksikön päällikkö Hilkka Nenonen ulkoasiainministeriö (1.8.2009 alkaen maahantuloasioiden koordinaattori Seija Haarala), tiimin vetäjä Jaana Honkakunnas ulkoasiainministeriö, projektipäällikkö Ismo Parviainen Poliisihallitus, poliisitarkastaja Timo Laine Poliisihallitus, ylitarkastaja Kimmo Pylväs Poliisihallitus, ylitarkastaja Jukka Hertell Poliisihallitus, ylitarkastaja Sari Kajantie, Keskusrikospoliisi, tutkija Kari Kanto Keskusrikospoliisi sekä ylikonstaapeli Marko Forss Helsingin poliisilaitos. Työryhmän teknisenä sihteerinä on toiminut osastosihteeri Sini Kallonen sisäasiainministeriön poliisiosasto.

Ulkomaalaisasioita on käsitelty erillisissä ulkomaalaisteemakokouksissa, jotka ovat koostuneet erikseen kutsutuista ulkomaalaisasioiden asiantuntijoista.

Työryhmän työhön ovat osallistuneet asiantuntijoina seuraavat henkilöt: lupahallintopäällikkö Minna Gråsten Poliisihallitus, neuvotteleva virkamies Tiina Ferm SM, lakimies Gunveig Planting-Visa Kuluttajavirasto, ylitarkastaja Heikki Partanen tietosuojavaltuutetun toimisto, tulosalueen johtaja Hanna Helinko Maahanmuuttovirasto, ylitarkastaja Raisa Bernards Maahanmuuttovirasto, ylitarkastaja Marjo Mäkelä Maahanmuuttovirasto, hankejohtaja Hilkka Vanhatalo Maahanmuuttovirasto, tulosalueen johtaja Ulla Vainikka Maahanmuuttovirasto, ylitarkastaja Pia Salmela sisäasiainministeriön maahanmuutto-osasto, komisario Arvo Mäntykenttä Helsingin ulkomaalaispoliisi, ylitarkastaja Jukka Tukia Maahanmuuttovirasto, teknologiapäällikkö Olli Lehtoranta hallinnon tietotekniikkakeskus, toimistosihteeri Elina Lappalainen ulkoasiainministeriö,

kehityspäällikkö Kaj Välimäki Väestörekisterikeskus, lainsäädäntöneuvos Johanna Puiro sisäasiainministeriö sekä rikosinsinööri Petri Varjos keskusrikospoliisi.

2 Johdanto

Hankkeen tavoitteena oli laatia identiteettiohjelma, jossa kuvataan kattavasti henkilöllisyyden luomiseen liittyvä nykytila, kehitysnäkymät ja riskit sekä tuoda esille johtopäätökset ja toimenpidesuositukset.

Kokonaisuutena tarkastelun alla ovat olleet valtion tehtävät henkilöllisyyden luomisessa yhteiskunnassa sekä keinot, joilla valtio tulevaisuudessakin suojaa kansalaisten henkilöllisyyttä sekä perinteisessä että sähköisessä toimintaympäristössä.

Raportin kokonaisuus on laaja ja siksi siihen on tehty tarkkoja rajauksia.

Työryhmä on määritellyt ja koonnut raporttiin keskeisiä termejä. Raportissa esitellään miten henkilöllisyys Suomessa luodaan ja miten sitä suojataan. Raportissa käydään läpi erilaisia tunnistamistapoja, varmenteita ja tunnistamisasiakirjoja sekä niihin liittyviä riskejä. Raportti sisältää myös aiheeseen liittyvän monin osin uudistuneen säädöspohjan tarkastelun. Lisäksi raportissa on hieman avattu biometriaa ja sen kehitystä viranomaistoiminnassa pääosin vain tunnistamisasiakirjojen osalta. Kansainvälistä vertailua on tehty henkilökorttien osalta.

Ulkomaalaisia koskevin osin raportti on rajattu varmistamattomaan henkilöllisyyteen liittyvään terminologiaan, tunnistamisasiakirjoihin sekä turvapaikanhakijoiden asiointiin liittyvään tunnistamisongelmaan. Muilta osin ulkomaalaispuolta on jo selvitetty kattavasti Ulkomaalaisten rekisterikäytäntöjä selvittäneen työryhmän loppuraportissa (SM 013:002006).

Kansainvälisesti identiteettivarkaudet ovat muodostuneet vakavaksi ongelmaksi. Useat maat ovat ryhtyneet mittaviin toimenpiteisiin identiteettivarkauksien estämiseksi. Oletettavissa on, että tilanne heikkenee myös Suomessa ja myös Suomessa on syytä pohtia identiteettivarkauksien ennalta estäviä kansallisia ja kansainvälisiä toimia.

Työryhmän tehtävänä oli käytännönläheisesti kansalaisnäkökulmasta kartoittaa mahdollisia ongelmatilanteita koskien identiteettivarkautta, sen tutkimista ja uhrin asemaa.[1] Usealta taholta on ehdotettu identiteettivarkauksien kriminalisointia, mutta tarkempaa analyysia kokonaisuudesta ei ole tehty. Raportissa on määritelty erilaisia tekotyyppejä ja tuotu esiin ongelmakohtia mahdollisten jatkotoimien pohjaksi ja tueksi. Lisäksi on pohdittu identiteettivarkauksien torjuntakeinoja. Uhrin asemaan on kiinnitetty erityistä huomiota.

[1] Tietoverkkorikollisuutta on aikaisemmin käsitelty myös Sisäisen turvallisuuden ohjelmassa: Turvallinen elämä jokaiselle. Sisäasiainministeriön julkaisu 16/2008.

Koska ”identiteettivarkaus” on käsitteenä vielä jossain määrin täsmentymätön, työryhmä otti ensisijaiseksi tavoitteekseen kirjoittaa auki millaisia konkreettisia tekokokonaisuuksia ilmiön alle kuuluu, minkä kaltaista vahinkoa niistä aiheutuu sekä millaisia erityiskysymyksiä rikostorjunnan sekä henkilötietolain valvonnan yhteydessä on tullut esille.

Verkossa tapahtuvien identiteettivarkauksien osalta kyse on ennen kaikkea toimintaympäristön muutoksesta, joka koskettaa suurta ihmisjoukkoa ja viranomaiskenttää. Näin ollen kokonaisvaltainen henkilöllisyyden luomista, sen käyttämistä ja turvaamista koskeva esitys onkin tarpeen.

3 Henkilöllisyyden nykytila

Työryhmän työssä käytetään seuraavia termejä. Osa on jo voimassa olevassa lainsäädännössä käytössä olevia termejä ja osa on työryhmän itsensä tekemiä.

3.1 Määritelmiä

Henkilö (person) = ihmisyksilö

Henkilötieto = Kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi (henkilötietolaki 523/1999).

Henkilöllisyys = Ihmisyksilö ja häneen liitettyjen VTJ:n tietojen (nimi, henkilötunnus, kansalaisuus) muodostama kokonaisuus. Henkilöllisyys syntyy samalla hetkellä, kun viranomaisen tietojärjestelmään (VTJ) luodaan henkilöä koskeva tietue ja se yhdistetään tavalla tai toisella fyysiseen henkilöön. Henkilöllisyydelle on olennaista ajallinen jatkuvuus, ts. sitä ei luoda aina uudelleen, vaikka henkilötiedot voivat muuttuakin.

Henkilötunnus (hetu) = yksikäsitteinen tunniste, joka erottaa henkilön kaikista muista henkilöistä ja jonka yhteyteen muut henkilötiedot voidaan koota viranomaistoiminnassa. Henkilötunnus sisältää syntymäajan.

Sähköinen asiointitunnus (satu) = Väestörekisterikeskuksen luonnolliselle henkilölle myöntämässä varmenteessa oleva varmenteen haltijan yksilöivä tunnistetieto. Tällä ei tunnisteta sellaisenaan.

Identiteetti = Yläkäsite, joka sisältää kaiken sellaisen tiedon, jonka avulla identiteetin haltijat voidaan erotella toisistaan. Henkilötieto muodostaa osajoukon identiteettitiedosta, mutta kaikki identiteettitieto ei ole henkilötietolain tarkoittamaa henkilötietoa. Identiteetin haltija voi olla luonnollisen henkilön lisäksi oikeushenkilö tai jokin ryhmä, jolla ei ole erikseen määriteltyä oikeudellista asemaa. Erityisesti tietoverkossa identiteetti voi myös olla täysin virtuaalinen. Tällaista identiteettiä käytetään erottelemaan sosiaalisen median osallistujat toisistaan, mutta identiteetti ei ole helposti yhdistettävissä hahmon taustalla olevaan todelliseen luonnolliseen henkilöön. Englannin kielessä identity tarkoittaa henkilöllisyyttä. Suomen kielessä identiteetti ei kuitenkaan tarkoita aina henkilöllisyyttä. Identiteetillä tarkoitetaan perinteisesti psykologiassa esimerkiksi sukupuoli-identiteettiä tai kansallisidentiteettiä.

Sähköinen identiteettitieto = Identiteettitiedon osajoukko, joka kattaa tietoverkossa käsiteltävän identiteettitiedon. Tietoa käytetään tietoverkossa erottelemaan jokin kokonai-

suus muista vastaavista kokonaisuuksista. Sähköistä identiteettitietoa on siten esimerkiksi etätunnistamiseen ja -todentamiseen käytettävä tunnistetieto (käyttäjätunnus + salasana), luottokorttinumero, palveluun tiettynä hetkenä yhteyttä ottavan työaseman verkko-osoite tai tietyn keskustelupalstan tietty nimimerkki. Tunnistamistieto on yleensä henkilötietoa, mutta ei aina; esimerkiksi www-palvelun osoite on myös identiteettitietoa, sillä yrityksen www-sivun sisältö on lähtökohtaisesti juuri tämän nimenomaisen yrityksen eikä jonkin muun yrityksen nimissä julkaistua tietoa. Tässä raportissa keskitytään nimenomaan henkilötietoihin, eikä yrityksiä koskevien tietojen käsittelyyn.

Tunnistautuminen = On omatoiminen prosessi, jossa henkilö esittäytyy automaattiselle tunnistusjärjestelmälle ja todentaa esittäytymisensä jollakin keinolla. Tunnistautuminen on teko, jossa toimija on tunnistuksen kohde itse. Tunnistamisen taas hoitaa joku, joka ei ole itse tunnistuksen kohteena.

Tunnistaminen (identification) = 1) Viranomaistoiminnassa: Henkilöllisyyden toteaminen eli henkilön yhdistäminen tiettyyn olemassa olevaan henkilöllisyyteen. Voi tapahtua kahdella tavalla: i) henkilö esittäytyy, ja esittäytyminen todennetaan tavalla tai toisella. ii) henkilöltä otetaan biometrinen tunniste, ja henkilöllisyys todetaan vertaamalla tunnistetta johonkin henkilötietorekisteriin tallennettuihin tunnisteisiin. 2) Yleisemmin: toimijan yhdistäminen tiettyyn tunnukseen tai tunnisteeseen, jolla toimija esiintyy suhteessa toisiin toimijoihin esimerkiksi tietoverkoissa. Tunnistamisen kohde voi olla 1) aktiivinen (esittäytyminen), 2) passiivinen (vastahakoinen tai vainaja) tai 3) ei tiedä, että tunnistetaan. Vain aktiivisessa toiminnassa tunnistaminen alkaa esittäytymisestä.

Fyysisesti läsnä olevan henkilön tunnistaminen = henkilö tunnistetaan kasvokkain.

Etätunnistaminen= Identiteetin todentaminen sähköisissä tietoverkoissa. Yleiskäsite, joka kattaa sekä vahvan että heikon sähköisen tunnistamisen.

Todentaminen (verification) = Tiedon tai tahon aitouden varmistaminen. Eri yhteyksissä todennetaan esimerkiksi, onko järjestelmän käyttäjä tai viestikumppani se, joksi on esittäytynyt, tai onko viesti, passi tai muu asiakirja aito eli eheä ja alkuperäinen. Todentamiseen liittyy aina jokin väite: henkilö on esittäytynyt rouva A:ksi eli väittää olevansa rouva A, jolloin todentaminen on väitteen todenperäisyyden varmistamista esimerkiksi tunnistamisasiakirjan avulla. Vastaavasti passin esittäminen rajanylityspaikalla sisältää epäsuoran väitteen, että passi on aito ja oikean passinhaltijan hallussa

Tunnistamisasiakirjat = tunnistamisessa yleisesti käytettäviä asiakirjoja. Esimerkiksi passi, henkilökortti, ajokortti, Kela-kortti jne.

Henkilöllisyyttä osoittava asiakirja = Valtioneuvoston asetuksessa poliisin myöntämistä henkilöllisyyttä osoittavista asiakirjoista (707/2006), 1 §:ssä todetaan, että poliisin myöntämiä henkilöllisyyttä osoittavia asiakirjoja, jotka hyväksytään tunnistamisasiakirjana henkilökorttia ja passia haettaessa, ovat henkilökorttilain (829/1999) 1 §:n 1 ja 3

momentissa tarkoitettu voimassa oleva henkilökortti ja passilain (671/2006) 3 §:ssä tarkoitettu voimassa oleva passi (Viittaus henkilökorttilain (289/1999) 6 §:n 2 mom.).

Vahva sähköinen tunnistaminen = Henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttämällä perustuen vähintään kahteen seuraavista kolmesta vaihtoehdosta: a) salasanaan tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltija tietää; b) sirukorttiin tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltijalla on hallussaan; tai c) sormenjälkeen tai johonkin muuhun tunnistusvälineen haltijan yksilöivään ominaisuuteen. (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009).

Heikko sähköinen tunnistaminen = Muu sähköinen tunnistaminen, joka ei täytä vahvan sähköisen tunnistamisen vaatimuksia.

Biometrinen tunniste = Yksilöllinen fyysinen ominaisuus tai käyttäytymispiirre, jonka perusteella henkilö voidaan tunnistaa. Yleisimpiä biometrisessä tunnistamisessa käytettyjä fyysisiä ominaisuuksia ovat kasvonpiirteet, sormenjäljet, kämmenen muoto, iiris, verkkokalvo ja ääni. Myös käyttäytymispiirteitä kuten kävelytyyliä tai huulten liikedynamiikkaa voidaan käyttää. Hyvän biometrisen tunnisteen tulee muuttua mahdollisimman hitaasti ja yksilöidä henkilö mahdollisimman tarkasti.

Biometrinen tunnistaminen = Henkilön tunnistaminen, joka perustuu biometrisiin tunnisteisiin. Vertaillaan asiakirjan haltijan fyysisiä ominaisuuksia esim. passiin tallennettuihin biometrisiin tunnisteisiin.

Varmenne = sähköinen todistus, joka todentaa henkilöllisyyden tai todentaa henkilöllisyyden ja liittää allekirjoituksen todentamistiedot allekirjoittajaan ja jota voidaan käyttää vahvassa sähköisessä tunnistamisessa sekä sähköisessä allekirjoituksessa. (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009)

Laatuvarmenne = on yksi sähköisen allekirjoituksen tyyppi. Laatuvarmenteella tarkoitetaan varmennetta, joka täyttää 2 momentissa säädetyt vaatimukset ja jonka on myöntänyt 33–38 §:ssä säädetyt vaatimukset täyttävä varmentaja. Laatuvarmenteen tulee sisältää: 1) tieto siitä, että varmenne on laatuvarmenne, 2) tieto varmentajasta ja sen sijoittautumisvaltiosta, 3) allekirjoittajan nimi tai salanimi, josta ilmenee, että se on salanimi, 4) allekirjoituksen todentamistiedot, jotka vastaavat allekirjoittajan hallinnassa olevia allekirjoituksen luomistietoja, 5) laatuvarmenteen voimassaoloaika, 6) laatuvarmenteen yksilöivä tunnus, 7) varmentajan kehittynyt sähköinen allekirjoitus, 8) mahdolliset laatuvarmenteen käyttörajoitukset; sekä 9) allekirjoittajaan liittyvät erityiset tiedot, jos ne ovat tarpeen laatuvarmenteen käyttötarkoituksen kannalta. (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009)

Kansalaisvarmenne = Kansalaisvarmenteella tarkoitetaan Väestörekisterikeskuksen luonnolliselle henkilölle myöntämää varmennetta, joka sisältyy henkilökorttilaissa

(829/1999) tarkoitettuun henkilökorttiin tai muuhun siihen verrattavaan viranomaisen asiakirjaan tai tekniseen alustaan, ja jota käytetään henkilön todentamista, sähköisen allekirjoituksen tekemistä sekä asiakirjojen ja viestien salausta varten. Kansalaisvarmenteella tarkoitetaan myös muuhun viranomaisen asiakirjaan tai tekniseen alustaan sisältyvää Väestörekisterikeskuksen myöntämää varmennetta, jota käytetään edellä mainittuun tarkoitukseen ja joka täyttää lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 30 §:ssä asetetut vaatimukset. (Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 661/2009).

Vahvan sähköisen tunnistamisen väline = esineitä ja yksilöiviä tietoja tai ominaisuuksia, jotka yhdessä muodostavat vahvaan sähköiseen tunnistamiseen tarvittavat tunnisteet, tunnistamisen välineet ja todentamisen välineet (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009).

Identiteettivarkaus = (engl. an identity theft) on yleisesti yleiskielessä käytetty käsite joukolle erilaisia tekokokonaisuuksia, joissa identiteettitietoa sekä kerätään että käytetään oikeudetta joko rikoshyödyn hankkimiseksi tai tavalla, josta aiheutuu identiteetin haltijalle vahinkoa tai muuten loukkaa uhrin oikeusturvaa. Identiteettivarkauden käsitteen tulisi kattaa myös teot, jotka loukkaavat henkilön itsemääräämisoikeutta aiheuttamatta selkeätä vahinkoa tai haittaa. Identiteettivarkaus on nimityksenä jossain määrin harhaanjohtava, sillä toisin kuin varkausrikoksessa (RL 28:1), identiteettivarkaudessa identiteettiä ei välttämättä oteta pois rikosuhrin hallusta. Rikoksentekijä vain kopioi tiedon myös omaan käyttöönsä. Termi on heikkouksista huolimatta niin laajalti käytetty, että työryhmäkin katsoi parhaaksi käyttää sitä.

Henkilöllisyysvarkaus = on puolestaan identiteettivarkauden osajoukko, jossa teko kohdistuu luonnolliseen henkilöön ja jossa kerättävä tieto on henkilötietoa.

Julkinen hallintotehtävä = Julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle (perustuslain 124 §)

3.2 Henkilöllisyyden luominen

Henkilöllisyyttä on kansainvälisesti tarkasteltu esimerkiksi henkilöllisyyden eri peruselementtien kautta:

1. biometrinen identiteetti; tekijät, jotka ovat yksilöillä ainutlaatuisia kuten sormenjäljet, ääni, kasvonmuoto, DNA jne.

2. annettu / luotu identiteetti; tekijät, jotka yksilö saa / annetaan syntyessään kuten nimi, syntymäaika- ja paikka, vanhempien nimet, kansalaisuus/kansalaisuudet jne.

3. elämänkerrallinen / historiallinen identiteetti; tekijät, jotka muodostuva elämän varrella kuten syntymän rekisteröinti, koulutodistukset, työhistoria, avioliittotiedot jne.

Suomessa henkilöllisyys muodostuu käytännössä syntymän tai maahanmuuton kautta kun henkilö merkitään väestötietojärjestelmään (VTJ). Suomessa on yksi maailman parhaista ja kattavimmista väestötietojärjestelmistä. Väestötietojärjestelmällä on pitkä historia, sillä väestötietoja on rekisteröity jo 1530-luvulta lähtien.

Suomessa jokaisella Suomen kansalaisella on oikeus viranomaisen antamaan henkilöllisyyteen. Henkilöillä on myös itsemääräämisoikeus ja omistusoikeus omiin tietoihinsa. Väestötietojärjestelmän osalta henkilön tietojen muuttamisen on perustuttava luotettavaan asiakirjaselvitykseen. Henkilöllä ei ole kuitenkaan oikeutta määrätä tietojensa rekisterissä pitämisestä tai niiden luovuttamisesta.

Väestötietojärjestelmä on valtakunnallinen rekisteri, jossa on perustiedot Suomen kansalaisista ja ulkomaalaisista, joilla on kotikunta Suomessa, rakennuksista, rakennushankkeista ja huoneistoista. Lisäksi järjestelmä sisältää kiinteistö- ja toimialatietoja ja tietoja vailla kotikuntaa rekisteröidyistä ulkomaalaisista. Väestötietojärjestelmää ylläpitävät Väestörekisterikeskus ja maistraatit. Tietoja käytetään hyväksi koko yhteiskunnan tietohuollossa, esimerkiksi julkishallinnossa, vaalien järjestämisessä, tutkimuksessa ja tilastoinnissa, verotuksessa sekä eläkejärjestelmissä. Maistraatti tallentaa tiedot ja muutokset omalta toimialueeltaan.

Uutta 1.3.2010 voimaan tullutta lakia väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009) sovelletaan väestötietojärjestelmän, sen tietojen ja palvelujen sekä Väestörekisterikeskuksen varmennetun sähköisen asioinnin ja sen palvelujen ylläpitämiseen, hyväksikäyttämiseen ja kehittämiseen. Väestötietojärjestelmän henkilötiedot nauttivat julkista luotettavuutta. Väestötietojärjestelmään henkilöstä talletettuja (13 §:n 1 momentin 1–21 kohdat) henkilötietoja pidetään julkisesti luotettavina tietoina, jollei osoiteta, että tieto on virheellinen tai puutteellinen.

Väestötietojärjestelmään talletetaan rekisteröinnin kohteena olevasta henkilöstä lähtökohtaisesti seuraavat tiedot:
1) täydellinen nimi, 2) henkilötunnus sekä tekninen tunnistetieto ja sähköinen asiointitunnus, 3) kotikunta ja siellä oleva asuinpaikka, tilapäinen asuinpaikka sekä sellaiset tiedot kiinteistöstä, rakennuksesta ja huoneistosta, jotka yksilöivät henkilön kotikunnan ja siellä olevan asuinpaikan, 4) vanhempien täydelliset nimet ja henkilötunnukset, 5) siviilisääty sekä tieto avioliiton solmimisesta ja purkautumisesta tai parisuhteen rekisteröinnistä ja rekisteröidyn parisuhteen purkautumisesta, 6) aviopuolison tai rekisteröidyn

parisuhteen toisen osapuolen täydellinen nimi ja henkilötunnus, 7) lasten täydelliset nimet ja henkilötunnukset, 8) lapsen ja vanhemman perheoikeudellista asemaa koskevat tiedot, 9) lapsen huoltoa ja sen sisältöä koskevat tiedot, 10) vahvistettua ottolapsisuhdetta koskevat tiedot, 11) toimintakelpoisuuden rajoittamista, edunvalvontaa ja edunvalvontavaltuutusta koskevat tiedot sekä edunvalvojan tai valtuutetun yksilöintitiedot, 12) lapsen huostaanottoa koskevat tiedot, 13) syntymäkotikunta tai -paikka ja syntymävaltio, 14) kansalaisuus, 15) transseksuaalin sukupuolen vahvistamista koskeva tieto, 16) kuolinaikaa tai kuolleeksi julistamisaikaa koskeva tieto, 17) paikallista rekisteriviranomaista koskevat tiedot, 18) vaalien ja kansanäänestysten toimittamista varten tarvittavat tiedot ääni- ja äänestysoikeudesta, 19) tieto jäsenyydestä uskonnonvapauslaissa (453/2003) tarkoitetussa uskonnollisessa yhdyskunnassa, 20) henkilön ilmoittama äidinkieli ja asiointikieli, 21) henkilötietolain ja tämän lain nojalla ilmoitetut rajoitukset luovuttaa väestötietojärjestelmän tietoja; sekä 22) henkilön ilmoittama postiosoite ja muu yhteystieto sekä ammatti.

3.2.1 Syntymä

Henkilöllisyys syntyy Suomen kansalaisten osalta henkilön syntyessä, kun henkilön tiedot viedään väestötietojärjestelmään. Väestötietojärjestelmä sisältää tiedot Suomessa pysyvästi asuvista henkilöistä sekä tietyistä väliaikaisesti asuvista henkilöistä.

Lapsen synnyttyä elävänä, hänet kirjataan väestötietojärjestelmään. Lapsen syntymästä ovat velvollisia ilmoittamaan a) terveydenhuollon toimintayksikkö, jossa synnytys on tapahtunut, b) terveydenhuollon ammattihenkilö eli lääkäri, kätilö, terveydenhoitaja tai sairaanhoitaja, joka on avustanut muualla kuin terveydenhuollon toimintayksikössä tapahtuneessa synnytyksessä ja c) lapsen äiti tai se, jonka hoidossa lapsi on, ovat velvollisia ilmoittamaan muusta kuin a)- ja b)-kohdissa mainituissa olosuhteissa syntyneestä lapsesta terveydenhuollon toimintayksikölle tai ammattihenkilölle.

Ilmoitus lapsen syntymästä väestötietojärjestelmään on tehtävä viimeistään synnytystä seuraavana päivänä. Edellä c)-kohdassa mainitun lapsen syntymästä ovat terveydenhuollon toimintayksikkö tai ammattihenkilö velvollisia ilmoittamaan viimeistään seuraavana päivänä siitä, kun tieto lapsen syntymästä on saatu äidiltä tai siltä, jonka hoidossa lapsi on.

Tieto lapsen syntymästä ilmoitetaan teknisen käyttöyhteyden avulla tai sähköisesti väestötietojärjestelmään merkittäväksi, jos lapsen äidillä on kotikunta Suomessa ja suomalainen henkilötunnus. Lapsen syntymän konekielistä ilmoittamista varten ilmoittaja tarvitsee joko maistraatin tai Väestörekisterikeskuksen myöntämän luvan. Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 26 §:n mukaan Väestörekisterikeskus antaa aina luvan tietojen ilmoittamiselle teknisen käyttöyhteyden avulla tai sähköisesti.

Muissa tapauksissa ilmoittaja toimittaa täytetyn lomakkeen maistraatille, jonka toimialueella lapsen äidillä on kotikuntansa. Jos lapsen äidillä ei ole kotikuntaa Suomessa tai se ei ole tiedossa, lähetetään ilmoitus maistraatille, jonka toimialueella lapsen syntymäkunta on. Kirjallista ilmoitusta varten on olemassa Väestörekisterikeskuksen vahvistama ja painattama lomake.

Lapsesta ilmoitetaan tässä vaiheessa syntymäpäivä, sukupuoli ja järjestyskirjain. Järjestyskirjaimen avulla yksilöidään lapset monisikiöisissä syntymissä.

Suomeen ulkomailta adoptoitu lapsi merkitään väestötietojärjestelmään joko hänen adoptiopäätöksen perusteella saamansa Suomen kansalaisuuden perusteella tai hänen saadessaan Suomesta kotikunnan ennen adoption loppuun saattamista. Lähtökohtaisesti lapsen väestötietojärjestelmään rekisteröinnin edellytyksenä on, että hänet tunnistetaan maistraatissa henkilökohtaisesti omasta matkustusasiakirjastaan.

Suomen kansalaisella voi olla vain yksi henkilöllisyys, mutta useita identiteettejä. Henkilöllisyys syntyy, kun henkilön tiedot viedään väestötietojärjestelmään. Suomessa on kattava väestötietojärjestelmä ja täten kansalaisilla on valtion takaama henkilöllisyys.

3.2.2 Maahanmuutto

Ulkomaalaiset henkilöt osoittavat henkilöllisyytensä Suomessa pääsääntöisesti kotivaltionsa myöntämällä, voimassa olevalla, matkustusasiakirjalla. Suomessa oleskeluluvalla oleskelevat ulkomaalaiset rekisteröivät henkilötietonsa väestötietojärjestelmään. Maistraatin hyväksyessä rekisteröitymisen ulkomaalaisen tiedot merkitään väestötietojärjestelmään ja hän saa henkilötunnuksen. Rekisteröimisen ja henkilötunnuksen perusteella ulkomaalaisen henkilöllisyys yksilöidään ja vahvistetaan Suomessa vastaavalla tavalla kuin Suomen kansalaisen osalta.

Tähän kirjaukseen ulkomaalainen henkilö tarvitsee asiakirjat, joista hänen henkilöllisyytensä ilmenee. Tilapäisesti Suomessa oleskelevat ulkomaalaiset voivat myös jättää kirjaamispyynnön Kansaneläkelaitokselle tai verottajalle, joka toimittaa tiedot maistraatille, joka kirjaa henkilön harkintansa mukaan väestötietojärjestelmään. Myös muiden tietojen kuten perhesuhdetietojen perustaksi maistraatti tarvitsee viralliset suomeksi käännetyt asiakirjat.

Ulkomaalainen voi pyytää tietojensa rekisteröimistä myös Maahanmuuttoviraston kautta oleskeluluvan hakemisen yhteydessä vastaavasti kuten Kansaneläkelaitoksen ja verottajan tapauksessa heidän tarpeitansa varten. Maistraatti hyväksyy myös nämä tiedot. Tiedot koskevat vain henkilöllisyyden perustietoja (sukunimi, etunimet, syntymäaika ja käytössä oleva kansalaisuus). Muut tiedot asianosainen käy ilmoittamassa maistraattiin.

Valtioneuvoston asetuksessa väestötietojärjestelmästä (128/2010) 20 §:ssä säädetään ulkomaan kansalaisesta väestötietojärjestelmään talletettavissa tiedoista. Ulkomaan kan-

salaisesta, joka oleskelee Suomessa tilapäisesti, voidaan tallettaa täydellinen nimi, sukupuoli, henkilötunnus, äidinkieli, kansalaisuus, osoite Suomessa, tilapäisen oleskelun alkamis- ja päättymispäivä sekä ne muut tiedot, jotka hän on ilmoittanut maistraatille.

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain keskeinen sisältö henkilöllisyyden kannalta on ulkomaalaisia koskevien rekisteröintikäytäntöjen uudistaminen. Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 9 § koskee edellytyksiä, joiden täyttyessä ulkomaan kansalaista koskevat tiedot voitaisiin rekisteröidä väestötietojärjestelmään. Ulkomaan kansalaista koskevat tiedot talletetaan väestötietojärjestelmään, jos hänellä on Suomessa kotikuntalain (201/1994) mukaan määräytynyt kotikunta ja siellä oleva asuinpaikka.

Muuta ulkomaan kansalaista koskevat tiedot voidaan tallettaa väestötietojärjestelmään, jos:

1. hänellä on Suomessa kotikuntalaissa tarkoitettu tilapäinen asuinpaikka ja tallettaminen on tarpeen työskentelyyn, opiskeluun tai muuhun vastaavaan olosuhteeseen liittyvien velvollisuuksien tai oikeuksien toteuttamisen vuoksi;
2. tallettaminen johtuu Suomea sitovan kansainvälisen sopimuksen velvoitteiden täyttämisestä; tai
3. tallettaminen on hänelle kuuluvien oikeuksien tai hänelle asetettujen velvollisuuksien toteuttamisen tai muun vastaavan erityisen ja perustellun syyn vuoksi välttämätöntä.

Säännös ei siis anna vailla kotikuntaa olevalle ulkomaan kansalaiselle ehdotonta oikeutta tulla rekisteröidyksi Suomen väestötietojärjestelmään. Maistraatin on varmistuttava pyynnön esittäjän henkilöllisyydestä voimassa olevasta matkustusasiakirjasta tai muusta vastaavasta luotettavasta asiakirjasta.

3.2.2.1 Henkilötietojen muuttaminen

Ulkomaalaisella henkilöllä voi olla Suomessa vain yksi käytössä oleva henkilöllisyys, mutta useita muita ”piileviä” henkilöllisyyksiä, jotka voivat olla lähinnä muissa maissa yhtä aikaa käytettyjä tai entisiä henkilöllisyyksiä. Henkilöillä voi olla myös kaksois- tai useampia kansalaisuuksia yhtä aikaa voimassa. Jos henkilöllä on Suomen kansalaisuus, se on aina käytössä oleva kansalaisuus.

Väestötietojärjestelmässä henkilöllä on aina vain yksi voimassaoleva henkilöllisyys ja henkilötiedot. Jos henkilötietoja muutetaan, jäävät aiemmat henkilötiedot talteen väestötietojärjestelmän historiatietoihin. Näiden tietojen luovuttaminen on kuitenkin rajoitetumpaa kuin voimassaolevien tietojen.

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 10 § koskee ulkomaan kansalaista koskevien tietojen luotettavuuden varmistamista. Pykälän mukaan maistraatin on tarkistettava, mitä tietoja ulkomaan kansalaisesta on

talletettu ulkomaalaisrekisteristä annetussa laissa (1270/1997) tarkoitettuun ulkomaalaisrekisteriin, ennen kuin se päättää häntä koskevan henkilötiedon lisäämistä, muuttamista tai korjaamista koskevan rekisterimerkinnän tekemisestä väestötietojärjestelmään. Valtioneuvoston asetuksella voidaan antaa tarkempia säännöksiä tarkistettavista tiedoista ja tarkistamisvelvollisuuden laajuudesta.

Samaisen pykälän mukaan, jos ulkomaan kansalaisen maistraatille ilmoittamia tietoja ei ole talletettu ulkomaalaisrekisteriin tai tiedot poikkeavat ulkomaalaisrekisteriin talletetuista tiedoista, maistraatin on ennen rekisterimerkinnän tekemistä pyydettävä asiasta Maahanmuuttoviraston lausunto. Maahanmuuttoviraston on käsiteltävä asia ilman aiheetonta viivytystä.

Myös ulkomaalaisrekisterin korvaava ulkomaalaisasioiden sähköinen asiankäsittelyjärjestelmä (UMA) tuo parannusta henkilöllisyysasioiden käsittelyyn, koska se mahdollistaa ns. katkeamattoman virkatodistus-tyyppisen ketjun henkilön henkilöllisyyksistä ja henkilötiedoista. UMA-järjestelmä on otettu käyttöön 8.11.2010. UMA:ssa asiakkaan henkilöllisyydestä pidetään yllä historiatietoja. Jos henkilöllä suku- tai etunimet tai käytössä oleva kansalaisuus vaihtuvat normaalilla tavalla kuten avioliiton solmimisen tai etunimen vaihtumisen tai valtion nimen muuttumisen valtion jakautumisen, valtioiden yhtymisen yhteydessä nimille ja kansalaisuuksille annetaan luonneluokitus. Jos taas on ilmennyt, että henkilön on esimerkiksi havaittu sormenjälkien perusteella käyttäneen muissa maissa eri henkilöllisyystietoja, järjestelmään tehdään merkintä poikkeavasta henkilöllisyystiedosta luonteella ”Muu henkilöllisyys”. UMA:an merkitään myös tieto siitä, mistä tieto on peräisin eli tiedon lähde. Muu henkilöllisyys merkitään myös silloin, jos henkilö ilmoittaa itselleen uuden syntymäajan, syntymäpaikan tai syntymävaltion. Lisäksi UMA:ssa on historiatiedot kaikista henkilötietojen muutoksista, mutta vain UMA:n käyttöönoton jälkeiseltä ajalta.

3.2.2.2 Ulkomaalaisen varmistamaton henkilöllisyys

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 19 § säätelee järjestelmän tietojen luotettavuuden varmistamista.

> Jos väestötietojärjestelmään talletettavaksi ilmoitettu tieto perustuu ulkomaiseen asiakirjaan, voidaan julkisesti luotettavana tietona väestötietojärjestelmään tallettaa asiakirjan perusteella vain sellainen tieto, jonka luotettavuus on varmistettu alkuperäisestä virallisesta asiakirjasta tai sen luotettavasti oikeaksi todistetusta jäljennöksestä taikka tiedon luotettavuus on aiemmin varmistettu suomalaisessa tuomioistuin- tai hallintomenettelyssä. Tässä tarkoitetun asiakirjan on oltava laillistettu tai siihen on liitettävä asianomaisen valtion toimivaltaisen viranomaisen todistus sen alkuperästä, jollei Suomea sitovan kansainvälisen sopimuksen velvoitteiden täyttämisestä muuta johdu. Ulkomaisen asiakirjan esittäjä on velvollinen tarvittaessa huolehtimaan esittämänsä asiakirjan kääntämisestä suomen tai ruotsin kielelle sekä sen laillistamisesta. Maistraatti voi tarvittaessa pyytää ulkoasiainministeriön, Maahanmuuttoviraston tai poliisiviranomaisen lausunnon edellä tarkoitetun asiakirjan aitoudesta ja luotettavuudesta.
>
> Väestötietojärjestelmään talletettuja tietoja on tarkistettava säännöllisesti niiden ajantasaisuuden ja luotettavuuden varmistamiseksi. Väestörekisterikeskus antaa tarkempia

määräyksiä tarkistettavista tiedoista sekä tarkistuksen toteuttamismenetelmistä ja -ajankohdasta.

Lähtökohtaisesti henkilön tunnistaminen luotettavasta matkustusasiakirjasta tai muusta vastaavasta asiakirjasta on väestötietojärjestelmään rekisteröinnin edellytys. Jossakin vaiheessa (viimeistään kotikunnan saadessaan) ulkomaalaisen toimiminen suomalaisessa yhteiskunnassa edellyttää kuitenkin väestötietojärjestelmään rekisteröintiä ja tällöin on luotettavan asiakirjaselvityksen puuttuessa tyydyttävä siihen, että hänestä rekisteröidään vastaavat tiedot kuin hänestä on ulkomaalaisrekisteriin tallennettu. Väestötietojärjestelmään ei ole mahdollista tehdä merkintää siitä, että järjestelmään merkityn henkilön henkilöllisyyttä ei ole voitu varmistaa. Väestötietojärjestelmään talletettuja henkilötietoja pidetään väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 18 §:n mukaan julkisesti luotettavina tietoina, jollei osoiteta, että tieto on virheellinen tai puutteellinen. Käytännössä väestötietojärjestelmään rekisteröidään kaikki nekin maassa vakinaisesti asuvat ulkomaalaiset, joiden henkilöllisyyttä ja henkilötietoja ei ole luotettavasti pystytty varmistamaan.

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annettua lakia valmistellessa selvitettiin, voitaisiinko väestötietojärjestelmään tehdä merkintä siitä, ettei henkilön henkilöllisyyttä ja häntä koskevia henkilötietoja ole voitu luotettavasti varmistaa. Selvityksen perusteella päädyttiin siihen, ettei tällaisen merkinnän tekemiseen ole riittäviä perusteita. Tähän ratkaisuun vaikutti erityisesti se, että väestötietojärjestelmän tiedoilla on lainsäädäntöön perustuva julkinen luotettavuus ja järjestelmän tietojen käyttötarkoitus on hyvin laaja (lain 5 §). Lisäksi ratkaisuun vaikuttavia seikkoja olivat:

- Julkisen luotettavuuden heikentämistä tiedon varmistamattomuutta koskevalla merkinnällä pidettiin periaatteellisesti ongelmallisena.
- Tiedon varmistamattomuutta koskevan merkinnän sisällön ja laajuuden määrittelyyn liittyi lainsäädännöllisiä ja käytännön ongelmia.
- Tiedon varmistamattomuutta koskevan merkinnän käsittelyyn rekisterihallinnossa (tekeminen ja ylläpito) liittyi toiminnallisia ja teknisiä ongelmia.
- Tiedon varmistamattomuutta koskevan merkinnän luovuttamiseen liittyi lainsäädännöllisiä ja teknisiä ongelmia.

Maahanmuuttoviraston arvioin mukaan jopa 80 % turvapaikanhakijoista ei esitä minkäänlaista henkilöllisyys- tai matkustusasiakirjaa maahan tullessaan. Turvapaikkaprosessi on nykyisellään pitkäkestoinen. Valitusprosessi mukaan lukien lopullisen lainvoimaisen turvapaikkapäätöksen syntyminen voi kestää jopa useita vuosia. Ilman henkilöllisyyden osoittavaa asiakirjaa olevalla turvapaikanhakijalla on mahdollisuus saada Suomen myöntämä, henkilötiedoilla varustettu asiakirja (muukalaispassi tai pakolaisen matkustusasiakirja) vasta siinä tapauksessa, jos hänelle myönnetään oleskelulupa. Suomessa oleskelee siis suuri määrä ulkomaalaisia ilman minkäänlaista asiakirjaa henkilöllisyydestään. Mainittu tilanne aiheuttaa ongelmia niin turvapaikanhakijoille itselleen, viranomaisille sekä palveluntarjoajille.

Viranomaisten kannalta ongelmana on, ettei turvapaikanhakijan henkilöllisyyttä pystytä jäädyttämään yhdeksi henkilöllisyydeksi heti turvapaikkaprosessin alusta lähtien. Hallitun turvapaikkaprosessin kannalta olisi tärkeää saada heti henkilölle luotua yksi identiteetti valtion näkökulmasta. Henkilöllisyyttä tai henkilöllisyyteen liittyviä henkilötietoja voitaisiin toki jälkikäteen muuttaa asianmukaisten dokumenttien avulla. Keskeistä on, ettei henkilöllä voi olla Suomen viranomaisen näkökulmasta katsottuna monta eri henkilöllisyyttä.

Turvapaikanhakijoiden kannalta ongelmaksi muodostuu turvapaikkaprosessin aikana se, että heillä tulisi olla mahdollisuus asioida esimerkiksi pankeissa, mutta tämä ei ole mahdollista pelkällä vastaanottokeskuksen antamalla pahvikortilla. Turvapaikanhakijoiden asiointi viranomaisissa on hankalaa ja sosiaalietuuksien maksaminen on vaikeaa. Turvapaikanhakijoiden toimeentulotuki joudutaan maksamaan käteisellä, mikä on omiaan vaarantamaan vastaanottokeskusten turvallisuutta. Käytännössä ”ilman henkilöllisyyttä” olevat turvapaikanhakijat voivat hoitaa pankki- ja muita asioitaan vain kuntien pakolaistyöntekijöiden tai muiden viranomaisten avulla.

Pankkeja koskeva laki rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä (503/2008) vaatii asiakkaan henkilöllisyyden varmistamista luotettavasta ja riippumattomasta lähteestä peräisin olevien asiakirjojen tai tietojen perusteella. Muukalaispassin tai pakolaisen matkustusasiakirjojen saamisen jälkeen käytännön asiointi yleisesti helpottuu, vaikka matkustusasiakirjoihin tehdään merkintä mahdollisesta varmistamattomasta henkilöllisyydestä.

Muutoin ulkomaalaisten rekisteröintiä on aikaisemmin kattavasti selvittänyt ulkomaalaisen rekisteröintikäytäntöjä selvittänyt työryhmä (SM 013:002006).

3.3 Henkilöllisyyden suojaaminen

3.3.1 Perustuslaki

Perustuslain (731/1999) 10 §:ssä säädetään yksityiselämän suojasta, joten yksityisyyden suojaamista voidaan pitää kansalaisen perustavaa laatua olevana oikeutena. Jollei erikseen ole muuta säädetty, henkilöllä on pääsääntöisesti oikeus hallita ja vallita omia henkilötietojaan ja päättää niiden käsittelystä. Yleislakina henkilötietojen käsittelyyn sovelletaan henkilötietolakia (523/1999). Valtioneuvoston periaatepäätöksessä sähköisestä tunnistamisesta on myös todettu, että henkilöllisyyden suojaamista voidaan pitää kansalaisen perustavaa laatua olevana oikeutena. Kansalaisen oikeusturvan kannalta on olennaista, että hänen henkilöllisyydestään pidetään huolta niin valtion, muiden toimijoiden kuin kansalaisen itsensäkin toimesta.

Perustuslain takaama yksityisyyden ja henkilötietojen suoja on vakiintunut merkittäväksi ja välttämättömäksi nykyaikaisen yhteiskunnan oikeudellisen sääntelyn osa-alueeksi.

Osa henkilön yksityisyyttä on hänen identiteettinsä, johon hänellä on tiedollinen itsemääräämisoikeus, joka on eräs itsemääräämisoikeutemme peruselementeistä. Tiedollinen itsemääräämisoikeus tarkoittaa yksilön pääsääntöistä oikeutta tietää omien tietojensa käsittelystä sekä oikeudesta vaikuttaa niiden käsittelyyn. Tiedollinen omistusoikeus eli oikeus omaan nimeen, kuvaan ja hahmoon ja niiden käyttämiseen koskee kaikkia. Myös sähköisen identiteettitiedon tulisi kuulua itsemääräämisoikeuden piiriin. Henkilöllä on lähtökohtaisesti oikeus säilyttää määräysvalta itseään koskevaan informaatioon, pitää se halutessaan salassa tai julkistaa se.

3.3.2 Julkisen vallan käyttö

Perustuslain 124 §:ssä säädetään hallintotehtävän antamisesta muulle kuin viranomaiselle. Julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle.

Henkilöllisyyttä osoittavien asiakirjojen osalta julkisen vallan käyttöala on selvä. Passin ja henkilökortin myöntämisen osalta kyse on hallintotoiminnasta ja merkittävästä julkisen vallan käytöstä. Henkilöllisyyttä osoittavien asiakirjojen myöntäminen on osa viranomaisen ydintehtävää eikä sitä voida siirtää yksityiselle toimijalle. Passi ja henkilökortti ovat valtion takaamia henkilöllisyyttä osoittavia asiakirjoja ja ne myönnetään poliisin toimesta.

Ajokortin osalta ajo-oikeusmenettelyiden arviointi ja kehittäminen -työryhmän muistiossa[2] (annettu 13.10.2009) otetaan kantaa ajokortin myöntämisen suhteeseen julkisen vallan käyttöön. Muistiossa todetaan, että myös ajo-oikeusmenettely on julkinen hallintotehtävä. Epäselvempää on, onko ajo-oikeuden myöntäminen merkittävää julkisen vallan käyttöä. Luvan peruuttaminen sen sijaan on merkittävää julkisen vallan käyttöä.

Sähköisten varmenteiden osalta tilanne on erilainen. Kansalaisvarmenteen myöntäminen on edelleen julkisen vallan käyttöä. Kansalaisvarmenne rinnastetaan tältä osin passiin tai henkilökorttiin.

> HE 89/2009 laiksi väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista. Tavoitteet: Tietoyhteiskunnan ja turvallisen sähköisen asioinnin perusedellytysten takaaminen sekä sähköisessä asiointitapahtumassa tarvittavan sähköisen henkilöllisyyden luominen kansalaisille ovat luonteeltaan sellaisia yhteiskunnan perustoimintoihin kuuluvia tehtäviä, joiden hoitaminen tulisi olla julkisen vallan vastuulla. Tätä näkökantaa puoltavat myös toiminnan jatkuvuuden turvaamiseen ja puolueettomuuteen liittyvät seikat. Tällaisessa toiminnassa on lisäksi kysymys teknisesti erittäin monimutkaisesta ja kustannusraskaasta toiminnasta sekä vaikeasti hallittavasta toimintaympäristöstä, johon saattaa liittyä tavanomaista liiketaloudellista riskiä suurempia epävarmuustekijöitä. Tämän johdosta esityksellä pyritään yksinkertaistamaan ja selkiyttämään jul-

[2] Ajo-oikeusmenettelyiden arviointi ja kehittäminen -työryhmän muistio (SMDno/2009/1431), 2009.

kishallinnon varmennettuun sähköiseen asiointiin liittyvien palvelujen kehittämistä sekä sähköisten asiointipalvelujen tarjoamiseen ja hyväksikäyttöön liittyvien tukipalvelujen tuottamista.

Muiden laatuvarmenteiden ja vahvan sähköisen tunnistamisen välineiden liikkeelle laskemisen ei sen sijaan katsota olevan julkisen vallan käyttöä. Tosin niidenkin osalta ensitunnistaminen perustuu viranomaisen myöntämiin asiakirjoihin. Näiden varmenteiden osalta tulkinta on siis muuttunut.

Perustuslakivaliokunta katsoi vielä (PeVL 2/2002) lain sähköisistä allekirjoituksista (14/2003) valiokuntakäsittelyssä, että laatuvarmenteiden tarjoamista on varmenteiden oikeusvaikutusten takia pidettävä perustuslain 124 §:n mukaisena julkisena hallintotehtävänä.

Lain sähköisistä allekirjoituksista ja vahvasta sähköisestä tunnistamisesta (617/2009) valiokuntakäsittelyssä perustuslakivaliokunta (PeVL 16/2009) päätyi toisenlaiseen lopputulokseen:

PeVL 16/2009: Perustuslakivaliokunta on arvioinut sähköisistä allekirjoituksista annetun lain tarkoittamaa laatuvarmenteiden tarjoamista perustuslain 124 §:n kannalta lausunnossaan PeVL 2/2002 vp. Tuolloin valiokunta katsoi laatuvarmenteen rinnastuvan viranomaisen myöntämään henkilötodistukseen, koska oikeustoimen edellytykseksi laissa säädetty allekirjoitus voidaan tehdä laatuvarmenteeseen perustuvaa sähköistä allekirjoitusta käyttämällä. Lisäksi valiokunta kiinnitti huomiota siihen, että varmennetoiminnalla on merkitystä sähköisen liiketoiminnan ja muun asioinnin osapuolten oikeusaseman kannalta. Laatuvarmenteiden tarjoamista oli siten valiokunnan mielestä varmenteen oikeusvaikutusten vuoksi pidettävä perustuslain 124 §:ssä tarkoitettuna julkisena hallintotehtävänä.

Sähköisestä allekirjoittamisesta annetussa laissa tarkoitettujen sähköisen allekirjoittamisen palveluiden ja laatuvarmenteiden levinneisyys ja käyttö on ollut Suomessa sittemmin hyvin vähäistä. Sähköisten allekirjoitusten asemesta tunnistamisen välineinä ovat käyttöön vakiintuneet pankkitunnukset, joita hallituksen arvion mukaan käytetään nykyisin noin 99 prosentissa tunnistustapahtumista. Nykyistä lakia sähköisistä allekirjoituksista ei sovelleta näihin tunnistuspalveluihin.

Ehdotetussa laissa on sen sijaan tarkoitus luoda puitteet tämänkaltaiselle yksityiselle palveluntarjonnalle. Lakiehdotuksessa tarkoitettujen liiketaloudellisten palvelujen luonne on valiokunnan mielestä siinä määrin etääntynyt julkiseen hallintotehtävään liitettävistä ominaispiirteistä, että toimintaa ei enää nykyisin ole pidettävä julkisena hallintotehtävänä, vaikka vahvan sähköisen tunnistamisen välineillä ja varmennetoiminnalla sinänsä onkin merkitystä erilaisissa oikeustoimissa osapuolten aseman kannalta. Näin ollen lakiehdotusta vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista ei ole tarpeen arvioida perustuslain 124 §:n kannalta.

Lakia koskevassa hallituksen esityksessä 36/2009 todetaan, että vahvan sähköisen tunnistamisen palvelun ja varmenteiden tarjonta ovat yksityistä palveluntarjontaa, johon ei ole tarvetta liittää perustuslain 124 §:n mukaista julkisen vallan käyttöä. Edes laatuvarmennetoiminta ei ole julkisen vallan käyttöä. Sen sijaan Väestörekisterikeskuksen kansalaisvarmenteita koskeva palveluntarjonta on julkisen vallan käyttöä. Tätä toimintaa koskee oma lakinsa, laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista. Siinä säädetään muun muassa kansalaisvarmennetta koskevasta erityisestä myöntämismenettelynsä, jossa poliisin suorittama henkilöllisyyden todentaminen on olennainen osa prosessia.

Myös Valtiontalouden tarkastusvirasto on tunnistuspalveluiden kehittämisestä ja käytöstä julkisessa hallinnossa antamassaan raportissa (161/2008) katsonut, että Väestörekisterikeskuksen kansalaisvarmennetoiminnassa on kyse viranomaistoiminnoista, kun taas muu laatuvarmenteiden tai muiden varmenteiden liikkeelle lasku ei tätä ole. Edellä sanottu tarkastelutavan muutos selkeyttää toimintakenttää olennaisesti. Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista säänneltäisiin puhtaasti yksityistä palveluntarjontaa, ja julkisen vallan käyttöä koskeva osuus sähköisten allekirjoitusten palveluiden tarjonnassa säännellään laissa väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista.

3.3.3 Toimivaltaiset viranomaiset

Fyysinen toimintaympäristö: Henkilöllisyyttä osoittavat asiakirjat eli passin ja henkilökortin myöntää poliisi. Ajokortin myöntää myös poliisi, vaikka se ei olekaan henkilöllisyyttä osoittava asiakirja. Henkilöllisyyttä osoittavien asiakirjojen myöntämisen ja tähän prosessiin liittyvän tunnistamisen osalta vastuuviranomainen on poliisi. Henkilöllisyyttä osoittavien asiakirjojen osalta lainsäädännöstä vastaa sisäasiainministeriö ja ajokorttien osalta liikenne- ja viestintäministeriö.

Sähköinen toimintaympäristö: Toimivaltaisten viranomaisten osalta tilanne on pirstaloitunut niin käytännön vastuun kuin lainsäädännönkin osalta. VM vastaa yleisestä valtion sähköisen toiminnan kehittämisestä, LVM vastaa vahvan sähköisen tunnistamisen ja sähköisten allekirjoitusten yleisestä kehittämisestä ja tietoyhteiskuntakehityksestä, poliisi myöntää henkilöllisyyttä osoittavat asiakirjat ja VRK VM:n alaisuudessa kansalaisvarmenteen. Valtioneuvoston periaatepäätöksessä sähköisestä tunnistamisesta on kaikkiaan 6 keskeistä ministeriötä: VM, LVM, OM, STM, SM ja TEM. Sähköinen tunnistaminen on asia, joka koskee kaikkia lähes kaikkia ministeriöitä, hallinnonaloja ja ihmis- ja organisaatioryhmiä.

3.4 Tunnistamisasiakirjat

Henkilöllisyyden osoittamisesta eri tilanteissa perinteisen, fyysisen henkilöllisyyden osalta ei ole olemassa lainsäädäntöä, mutta tilanne on kuitenkin vakiintunut. Valtioneuvoston asetuksessa poliisin myöntämistä henkilöllisyyttä osoittavista asiakirjoista (707/2006), 1 §:ssä todetaan, että poliisin myöntämiä henkilöllisyyttä osoittavia asiakirjoja, jotka hyväksytään tunnistamisasiakirjana henkilökorttia ja passia haettaessa, ovat henkilökorttilain (829/1999) 1 §:n 1 ja 3 momentissa tarkoitettu voimassa oleva henkilökortti ja passilain (671/2006) 3 §:ssä tarkoitettu voimassa oleva passi (Viittaus henkilökorttilain (289/1999) 6 §:n 2 mom.) Poliisin lakisääteinen perustehtävä on myöntää henkilöllisyyttä osoittavat asiakirjat. Toisin sanoen poliisin myöntämiä henkilöllisyyttä osoittavia asiakirjoja ovat vain henkilökortti ja passi. Myöntöprosessi on keskeinen osa passin ja henkilökortin luotettavuutta. Asiakirjan luotettavuus ei perustu pelkästään sen vaikeaan fyysiseen väärennettävyyteen vaan myös ja eritoten myöntöprosessin luotettavuuteen.

Passi ja henkilökortti ovat siis asetustasolla määriteltyjä henkilöllisyyttä osoittavia asiakirjoja. Virallinen henkilöllisyystodistus on vanha nimike, josta luovuttiin nimenomaisesti 1980-luvun lopussa, kun siirryttiin vanhoista paperisista henkilöllisyystodistuksista henkilökortteihin.

Poliisi myöntää myös ajokortin, mutta sen tehtävänä on ainoastaan osoittaa ajo-oikeuden olemassa olo, eikä se siten ole henkilöllisyyttä osoittava asiakirja. Käytännössä sitä käytetään kuitenkin yleisesti henkilöllisyyden osoittamisessa muun muassa pankeissa ja kaupoissa. Lisäksi henkilöllisyyden osoittamiseen käytetään myös kuvallista Kela-korttia. Kela-kortin myöntää Kansaneläkelaitos.

Henkilökortin myöntämisestä säädetään henkilökorttilaissa ja passin myöntämisestä passilaissa. Myöntöprosessissa poliisi tunnistaa henkilön luotettavasti ja myöntää turvatasoltaan korkeatasoisen, vaikeasti väärennettävän asiakirjan. Poliisi siis myöntää todistuksen henkilöllisyydestä. Passin ja henkilökortin tasoa on kohotettu erilaisin toimenpitein. Kansainvälisesti biometristen tunnisteiden käyttöönottaminen matkustusasiakirjoissa on kohottanut matkustusturvallisuutta sekä toimii tehokkaana väärinkäytöksiä ennalta estävänä tekijänä.

Henkilöllisyyttä osoittavien asiakirjojen osalta ei ole ollut olemassa yleistä lainsäädäntöä, jossa olisi määritelty hyväksyttävät tunnistamisasiakirjat. Vahvan sähköisen tunnistamisen osalta 1.9.2009 voimaan tullut laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) sääntelee vahvan sähköisen tunnistamisen välinettä haettaessa käytettävistä tunnistusasiakirjoista. Laissa määritellään, että vahvan sähköisen tunnistamisen välinettä haettaessa ensitunnistamisen yhteydessä voidaan käyttää tunnistamisasiakirjana passia, henkilökorttia ja valinnaisesti myös vuoden 1990 jälkeen myönnettyä ETA-maiden ajokorttia. Mahdollisuus käyttää ajokorttia ensitunnistamiseen oli lakia koskevassa hallituksen esityksessä määräaikainen, mutta eduskunta poisti määräaikaisuuden sen johdosta, että tosiasiallinen vallitseva käytäntö perustuu pitkälti ajokortin käyttöön.

Finanssisektorin osalta laki rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä (503/2008) ei määrittele käytettäviä asiakirjoja. Lain määritelmissä (5 §:n 5 kohta) todetaan kuitenkin, että henkilöllisyyden todentamisella tarkoitetaan asiakkaan henkilöllisyyden varmistamista luotettavasta ja riippumattomasta lähteestä peräisin olevien asiakirjojen tai tietojen perusteella. Lainsäädäntöä on tältä osin täydennetty erilaisilla ohjeilla. Näitä ovat finanssivalvonnan standardi 2.4 asiakkaan tunnistaminen ja tunteminen (Rahanpesun, terrorismin rahoituksen sekä markkinoiden väärinkäytösten estäminen, määräykset ja ohjeet) sekä pankkien sisäiseen käyttöön tarkoitettu Finanssialan keskusliiton asiakkaan tunnistusta koskeva opaskirja. Lähtökohtaisesti näissä ohjeissa hyväksyttyjä tunnistamisasiakirjoja ovat passi, henkilökortti, ajokortti ja kuvallinen Kela-kortti. Laissa väestötietojärjestelmästä ja Väestörekisterikeskuksen varmen-

nepalveluista (661/2009) mainitaan tunnistamisasiakirjoina poliisin myöntämät henkilöllisyyttä osoittavat asiakirjat.

Tunnistamisasiakirjoja käytetään erilaisissa tunnistamistapahtumissa. Tyypillisimpiä tunnistamistapahtumia ovat viranomaisasiointi, pankkiasiointi sekä erilaisen kaupanteon yhteydessä tehtävä tunnistaminen. Näissä tilanteissa tunnistamistahosta riippuen tunnistamisasiakirjana käytetään joko kaikkia tai joitakin seuraavia asiakirjoja: passia, henkilökorttia, ajokorttia ja Kela-korttia. Kauppojen asioinnin osalta on todettava, että uusilla sirullisilla maksukorteilla tunnistaudutaan PIN-koodilla, eikä näin ollen enää tunnistamisasiakirjaa tarvitse näyttää. Seuraavissa kappaleissa kerrotaan tunnistamiseen käytettävistä asiakirjoista.

3.4.1 Passit

Passilaki (671/2006) sääntelee passien myöntämistä. Neuvoston asetus (EY) 2252/2004 jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista (ns. EU-passiasetus) sääntelee biometristen tunnisteiden käyttöönottamista passeissa ja muissa matkustusasiakirjoissa. Ensimmäinen biometrinen tunniste, kasvokuva, otettiin Suomessa käyttöön elokuussa 2006 voimaan tulleella passilain muutoksella (671/2006), josta lähtien passeissa on ollut myös koneellisesti luettava tekninen osa eli siru. Kesäkuussa 2009 voimaan tulleella passilain muutoksella (456/2009) lisättiin passeihin toinen biometrinen tunniste, sormenjäljet.

Kyseisessä passilain muutoksessa (456/2009) keskeistä on sormenjälkitietojen siruun tallettaminen ja sormenjälkitietojen rekisteröinti. Passin siruun talletettuja sormenjälkiä saa lukea vain passin myöntämä viranomainen sekä poliisi- ja rajatarkastusviranomainen silloin, kun se on tarpeen henkilön tunnistamiseksi tai asiakirjan aitouden todentamiseksi passin hakemiseen ja matkustusoikeuden toteamiseen liittyvissä toiminnoissa. Poliisilla on lisäksi oikeus passin sirun sormenjälkien lukemiseen aina silloin, kun sillä on laissa säädetty oikeus varmentaa henkilön henkilöllisyys.

Rekisteröinnin tavoitteena on taata passinhakuprosessin turvallisuus ja henkilöllisyyden luotettava varmistaminen. Ehdotettu menettely edistää kansalaisten oikeusturvaa, koska henkilön tunnistaminen voidaan tehdä luotettavasti ja nopeasti sekä passia haettaessa että muissa tunnistustilanteissa. Rekisteröinnillä pyritään suojaamaan henkilön identiteettiä. Vertaamalla passinhakijan sormenjälkiä tietokannassa oleviin sormenjälkiin voidaan varmistua siitä, ettei henkilö hae passia useammalla henkilöllisyydellä tai että passi myönnetään hakijan tiedoilla vain yhdelle henkilölle. Tietokantaan talletetuilla sormenjäljillä voidaan varmistaa myös henkilön henkilöllisyys esimerkiksi tilanteessa, jossa hänen esittämänsä passin siru on rikki tai rikottu. Lisäksi henkilöllisyys kyetään varmistamaan siinä tapauksessa, että henkilöllä ei ole asiakirjan katoamisen tai muun syyn vuoksi esittää asiakirjaa todistukseksi henkilöllisyydestään.

Rekisteriin talletettuja passinhakijan sormenjälkitietoja voidaan käyttää henkilön henkilöllisyyden varmistamiseksi silloin, kun käyttötarve liittyy passinhakijan tunnistamiseen henkilön hakiessa passia tai passinhaltijan tunnistamiseen tilanteessa, jossa viranomaisella on henkilön matkustusoikeuteen, maastalähtöön ja maahantuloon liittyvä oikeus tarkastaa henkilön henkilöllisyys ja esitetyn asiakirjan aitous. Hakijalta otettua ja rekisteriin talletettua sormenjälkeä voidaan käyttää myös haetun asiakirjan valmistamiseksi.

Passin myöntämisessä on kyse henkilön osalta hänen perustuslaillisen liikkumisvapautensa toteuttamisesta ja näin ollen henkilöllä on subjektiivinen oikeus saada passi. Passia käytetään vain matkustamiseen ja henkilöllisyyden osoittamiseen. Normaali passi on voimassa 5 vuotta ja se sisältää biometrisen kasvokuvan ja sormenjäljet. Voimassa olevia passeja on noin neljä miljoonaa kappaletta.

Passihakemuksen voi jättää paikallispoliisin palvelupisteeseen millä tahansa paikkakunnalla. Ulkomailla asuva Suomen kansalainen voi hakea passia minkä tahansa Suomen edustuston passinmyöntöpisteestä, joita ovat suurlähetystöt, pääkonsulinvirastot ja lähetetyn konsulin johtamat edustustot eli konsulaatit. Ulkomailla asuva suomalainen voi jättää hakemuksen myös poliisilaitoksella Suomessa. Passihakemus on jätettävä henkilökohtaisesti, jolloin henkilöllisyys todistetaan passilla tai henkilökortilla. Mikäli passin hakijalla ei ole henkilöllisyyttä osoittavia asiakirjoja, selvitetään henkilöllisyys tutkinnallisin keinoin. Passiin merkitään vain yhden henkilön tiedot, lapsia ei siis voi merkitä huoltajan passiin. Passi maksetaan hakemusta jätettäessä ja valmiin passin voi noutaa myös asiamies tai se voidaan pyynnöstä lähettää hakijalle postitse.

Muukalaispassi ja pakolaisen matkustusasiakirja ovat kansallisen passin sijasta ulkomaalaisille annettavia matkustusasiakirjoja, joita voidaan käyttää henkilöllisyyttä osoittavina asiakirjoina, jollei niissä ei ole merkintää siitä, ettei matkustusasiakirjan haltijan henkilöllisyyttä ole pystytty varmistamaan. Muukalaispassin haltija saa palata ulkomailta Suomeen, jos passissa on siihen oikeuttava oleskelulupa, ja pakolaisen matkustusasiakirjan haltija niin kauan kuin asiakirja on voimassa. Jos muukalaispassin tai pakolaisen matkustusasiakirjan haltijan henkilöllisyyttä ei ole pystytty varmistamaan, tehdään siitä merkintä matkustusasiakirjaan. Henkilöllisyys voidaan varmistaa esimerkiksi luotettavalla kansallisella passilla tai henkilöllisyyttä osoittavalla asiakirjalla.

Maahanmuuttovirasto myöntää muukalaispassin ulkomaalaiselle, joka on saanut oleskeluluvan toissijaisen suojelun perusteella. Myös tilapäisen suojelun tarpeen perusteella oleskeluluvan saaneelle myönnetään muukalaispassi, jos hänellä ei ole voimassa olevaa matkustusasiakirjaa. Lisäksi muukalaispassi voidaan myöntää ulkomaalaiselle, jos hän ei voi saada passia kotimaansa viranomaiselta, on kansalaisuudeton tai muukalaispassin saamiselle on muu erityinen syy. Tällaisia syitä voivat olla esimerkiksi tarve matkustaa kotimaahan kansallisen passin saamiseksi tai se, ettei kansallista passia ole pystytty hankkimaan yrityksistä huolimatta. Muukalaispassi on voimassa enintään 5 vuotta. Uuden muukalaispassin myöntää tavallisesti asuinpaikkakunnan poliisi.

Maahanmuuttovirasto myöntää pakolaisen matkustusasiakirjan ulkomaalaiselle, joka on saanut pakolaisaseman eikä sitä ole lakkautettu tai peruutettu. Pakolaisen matkustusasiakirja on voimassa enintään 5 vuotta. Uuden matkustusasiakirjan myöntää tavallisesti asuinpaikkakunnan poliisi.

3.4.2 Henkilökortit

Henkilökorttiin hakijalla ei ole subjektiivista oikeutta. Henkilökortin voi saada siis vain, mikäli henkilöllisyys on voitu luotettavasti todentaa. Henkilökorttilain (829/1999) 1 §:ssä todetaan seuraavaa. ”Poliisi antaa hakemuksesta todistuksen henkilöllisyydestä (henkilökortti) Suomen kansalaiselle ja kotikuntalain (201/1994) mukaisesti Suomessa vakinaisesti asuvalla ulkomaalaiselle, joka on merkitty väestötietojärjestelmään ja jonka henkilöllisyys on voitu luotettavasti todeta.”

Poliisi myöntää henkilökortteja, alaikäisen henkilökortteja ja väliaikaisia henkilökortteja. Henkilökorttityyppejä ovat henkilökortti, väliaikainen henkilökortti, alaikäisen henkilökortti sekä ulkomaalaisen henkilökortti. Voimassa olevia henkilökortteja voi olla kerrallaan vain yksi. Kaikki henkilökortit ovat henkilöllisyyttä osoittavia asiakirjoja.

Henkilökorttihakemus voidaan jättää paikallispoliisin palvelupisteeseen. Henkilökorttihakemus on jätettävä henkilökohtaisesti ja se maksetaan hakemusta jätettäessä. Henkilökortin toimitusaika on noin kaksi viikkoa. Henkilökortti noudetaan joko henkilökohtaisesti poliisilaitokselta tai se lähetetään asiakkaalle postitse (asiakkaan valinnan mukaan kirjattuna tai tavallisena postina). Henkilökortin voi noutaa myös valtuutettu asiamies.

Henkilökortti ja alaikäisen henkilökortti ovat voimassa 5 vuotta ja väliaikainen henkilökortti enintään neljä kuukautta. Henkilökorttia haettaessa on oltava mukana 1 passikuva, luotettava selvitys henkilöllisyydestä (passi tai henkilökortti) ja mikäli hakija on alle 18-vuotias, huoltajien suostumus (paitsi ns. alaikäisen henkilökortti). Mikäli henkilöllä ei ole passia tai henkilökorttia mukanaan, suoritetaan erityinen tunnistamismenettely. Henkilökortin voi siis saada myös muun muassa ajokortin ja rekisterikyselyyhdistelmän kautta. Pelkällä ajokortilla passia tai henkilökorttia ei voi saada.

Poliisi voi myöntää ulkomaalaisen henkilökortin myös kotikuntalain mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle, joka on merkitty väestötietojärjestelmään ja jonka henkilöllisyys voidaan todeta luotettavasti. Hakumenettely on sama kuin muissakin henkilökorttityypeissä.

Henkilökortilla on eri käyttötarkoituksia. Henkilökorttia käytetään perinteiseen fyysiseen tunnistamiseen henkilöllisyyttä osoittavana asiakirjana ja lisäksi Suomen kansalaiset voivat käyttää korttia matkustusasiakirjana passin sijasta Euroopassa. Poikkeuksia ovat ilman huoltajien suostumusta alaikäiselle myönnetty ns. alaikäisen henkilökortti, ulkomaalaiselle myönnetty henkilökortti sekä väliaikainen henkilökortti, mitkä eivät

käy matkustusasiakirjana. Kadonneeksi tai anastetuksi ilmoitettua henkilökorttia ei voida käyttää matkustusasiakirjana sen löydyttyä, ennen kuin kortin omistaja on esittänyt kortin poliisille ja ilmoittanut sen löytymisestä.

Henkilökortteja on myönnetty noin 400 000 kappaletta. Myöntömäärät ovat kasvaneet vuosittain 10–12 %.

Henkilökorttilaki sääntelee henkilökorttien myöntämistä. Henkilökorttien sääntely ei ole ollut passeista poiketen EU-sääntelyä, vaan täysin kansallista, koska henkilökorteista sääntelemiselle ei ole ollut oikeusperustaa perustamissopimuksissa.

Lissabonin sopimuksella, joka tuli voimaan 1.12.2009, luotiin uusi oikeusperusta antaa EU-säädöksiä myös passeista, henkilötodistuksista, oleskeluluvista ja muista niihin rinnastettavista asiakirjoista. Henkilökorttien oikeusperustasta määrätään Lissabonin sopimuksen voimaantulon myötä Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) V osaston 2 luvun (rajavalvonta-, turvapaikka- ja maahanmuuttopolitiikka) 77 artiklan 3 kohdassa. Oleskelulupien osalta käytetään maahanmuuttopolitiikkaan liittyvää oikeusperustaa (SEUT 79 artiklan 2 kohta).

Uuden oikeusperustan mukaan, jos on osoittautunut, että tarvitaan unionin toimintaa helpottamaan mahdollisuutta käyttää SEUT 20 artiklan 2 kohdan a alakohdassa tarkoitettua unionin kansalaisen oikeutta liikkua ja oleskella vapaasti jäsenvaltioiden alueella, eikä perussopimuksissa ole määräyksiä tähän tarvittavista valtuuksista, neuvosto voi antaa erityistä lainsäätämisjärjestystä noudattaen säännöksiä, jotka koskevat passeja, henkilötodistuksia, oleskelulupia ja muita niihin rinnastettavia asiakirjoja. Neuvosto tekee ratkaisunsa yksimielisesti Euroopan parlamenttia kuultuaan. Aiemmin nämä kysymykset oli suljettu yhteisön toimivallan ulkopuolelle (Euroopan yhteisön perustamissopimus (SEY) 18 artikla 3 kohta). Tästä huolimatta esimerkiksi SEY 62 artiklan 2 kohdan a alakohdan nojalla on voitu yhdenmukaistaa jäsenvaltioiden myöntämien passien turvatekijät, mukaan lukien biometriset tunnisteet (neuvoston asetus (EY) N:o 2252/2004, annettu 13 päivänä joulukuuta 2004, jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista (EUVL L 385 2004, s. 1).

Lissabonin sopimuksen vaikutusta on vaikea arvioida, koska EU:n mahdollista lainsäädäntökehitystä on vaikea ennakoida. Jos ehdotuksia säännöksiksi passeista, henkilötodistuksista, oleskeluluvista ja niihin rinnastettavista asiakirjoista annetaan, niin niiden käsittelyaikaan ja lopulliseen sisältöön vaikuttaa muun muassa neuvoston yksimielisyyden vaatimus. Ennakoitavissa on, että kehitys lienee periaatteellisesti samanlaista passin kanssa, koska molemmat ovat matkustusasiakirjoja. Jo pelkällä oikeusperustalla on kuitenkin vaikutusta myös kansallisiin ratkaisuihin. Suurimmassa osassa EU-maita on menossa merkittäviä projekteja henkilökorttien osalta.

Jäsenvaltioiden hallitusten välinen päätelmä kansallisia henkilökortteja koskevista yhteisistä minimiturvatekijöistä hyväksyttiin joulukuussa 2005. Jäsenvaltioiden päätelmässä kiinnitetään huomiota myös henkilökorttien muihin turvatekijöihin kuin biometrisiin tunnisteisiin (materiaali, painatustekniikka ja kopioinnin estäminen), myöntämisprosessien turvallisuuteen sekä asiakirjojen turvalliseen säilytykseen ja kuljetukseen. Päätelmä ei ole ollut oikeudellisesti sitova eikä päätelmä ole sisältänyt määräaikoja sen noudattamiselle. Päätelmän suositusten soveltaminen on jäänyt kansallisten ratkaisujen varaan. Päätelmässä todetaan jäsenmaiden oikeus päättää itse henkilökorttien myöntämisestä sekä niihin liitettävistä biometrisista tunnisteista.

Päätelmän mukaan jäsenvaltioiden tulisi käyttää biometrisinä tunnisteina kasvokuvaa sekä kahta sormenjälkeä, kuten passeissa. Myös turvatekijöiden osalta noudatettaisiin samoja turvatekijöitä kuin passeissa soveltuvin osin. Myöntämisprosessin eri vaiheiden osalta esitetään vähimmäisvaatimuksia, joiden mukaisesti henkilön tulee ainakin kerran hakemusvaiheessa käydä henkilökohtaisesti viranomaisen luona. Hakemusvaiheessa tulee hakemukset tarkastaa tietojärjestelmien avulla sekä prosessien tulee olla valvottuja sekä prosessissa tulee olla mukana enemmän kuin yksi henkilö. Turvallisesta asiakirjojen säilytyksestä sekä kuljetuksesta tulee varmistua.

Suomi on jo nykyisellään minimiturvatekijöiden osalta noudattanut linjaa, jonka mukaisesti passin ja henkilökortin turvatekijät ovat samankaltaisia soveltuvin osin. Suomen nykyinen henkilökortti täyttää jo nykyisellään päätelmien minimiturvatekijät. Sen sijaan biometristen tunnisteiden lisääminen henkilökorttiin edellyttäisi henkilökorttilain muuttamista. Henkilökorttien myöntämisprosessi poliisin myöntämänä asiakirjana täyttää jo pääosin edellytetyt vaatimukset myöntämisprosessin turvallisuudelle.

Matkustusturvallisuuden lisäämiseksi sekä järjestäytyneen rikollisuuden sekä laittoman maahanmuuton torjumiseksi on tärkeää löytää ennalta estäviä keinoja. Suositusten antaminen henkilökorttien osalta lisää yhdenmukaisten turvatekijöiden käyttöä sekä myöntöprosesseja Euroopan unionin alueella. Tämä vaikuttaa myönteisesti henkilön identiteetin suojaamiseen sekä matkustusturvallisuuteen. Korttien turvatason noustessa, myöntöprosessin merkitys kasvaa ja se muodostuu ketjun heikoksi kohdaksi. Tämän vuoksi Euroopan unioni, G-8 -maat sekä ICAO ovat valmistelleet nimenomaisesti myöntöprosessia koskevia vähimmäisvaatimuksia. Vaatimukset koskevat matkustusasiakirjoja.[3]

Raportin liitteenä on lista henkilökortteja myöntävistä EU-maista. Asiakirjan tiedot on koonnut ulkoasiainministeriö edustustojensa kautta. Liitteestä käy ilmi, että henkilökortit ovat pakollisia varsin suuressa osassa EU-maita.

[3] ICAO, Guide for Assessing Security of Handling and Issuance of Travel Documents, 2010.

3.4.3 Ajokortit

Ajokortin malli, ajokorttiluokat, ajo-oikeuden saaminen ja kuljettajaopetus on harmonisoitu Euroopan unionissa ajokorttidirektiivissä, (91/439/ETY neuvoston direktiivi yhteisön ajokortista.) Se sääntelee ajokortin saamisen vähimmäisedellytyksiä, joita ovat mm. ajoneuvojen kuljettamiseen liittyvät tiedot sekä vaatimukset ajotaidolle ja ajotavalle. Lisäksi direktiivissä määritellään ajokorttiluokat. Itse ajokortin myöntämistä koskevia hallinnollisia menettelyitä direktiivi ei koske. Uusin ajokorttidirektiivi (2006/126/EY), Euroopan neuvoston ja parlamentin direktiivi ajokorteista on annettu 20.12.2006.

Ajokorttidirektiivin III -vaiheen on tultava kansallisesti voimaan viimeistään 19.1.2013. Liikenne- ja viestintäministeriö vastaa ajo-oikeutta ja ajokortteja koskevasta lainsäädännöstä. Säännökset sisältyvät tieliikennelakiin (267/1981, 5 luku) ja ajokorttiasetukseen 845/1990). Poliisin toimivallasta ajo-oikeusasioissa on säädetty tieliikennelain 82 ja 108 a §:ssä. Poliisihallitus antaa poliisille tarkempia ohjeita ja määräyksiä tieliikennelain ja sen nojalla annettujen säännösten mukaan poliisille kuuluvien tehtävien suorittamisesta. Ajokortin saamiseksi henkilön on haettava ajokorttilupaa: lupa pitää hakea ensimmäistä ajokorttia hankittaessa, mutta myös ajokorttia uudistettaessa ja ajokortin luokkaa korotettaessa.

Ajokorttihakemus tehdään kirjallisesti, mutta henkilökohtaista asiointia ei edellytetä. Nykyisin merkittävä osa hakemuksista jätetäänkin autokouluihin, jotka tarkistavat hakijan henkilöllisyyden ja toimittavat asiakirjat poliisille.

Suomalaisen ajokortin saamisen edellytyksenä on, että hakijan vakituinen asuinpaikka on Suomessa tai että hän on opiskellut Suomessa vähintään kuusi kuukautta ja opiskelu jatkuu edelleen. Jos henkilöllä ei ole väestötietojärjestelmän mukaan kotipaikkaa Suomessa, mutta hakija on kuitenkin sitä mieltä, että asuu vakinaisesti Suomessa, hänen tulee esittää asiasta selvitystä.

Poliisin myönnettyä luvan lyhytaikaisen ajokortin saamiseksi, hakemus lähetetään Liikenteen turvallisuusvirastolle, joka tallentaa tiedot tietojärjestelmään. Lyhytaikaisen kortin luovuttaa asiakkaalle kuljettajatutkinnon vastaanottaja. Muiden ajokorttilupahakemusten (esimerkiksi ajokorttiluokan korottamisten, ajokortin uudistamisten, mopo- tai moottoripyöräkortin tai ajokortti ulkomaisen ajokortin perusteella) tiedot poliisi tallentaa itse tietojärjestelmään. Varsinaisen ajokortin luovuttaa hakijalle hänen asuinpaikkansa poliisi.

Ajokortin tehtävänä on osoittaa ajo-oikeus ja todistaa tarvittaessa ajoneuvon kuljettajan henkilöllisyys ajoneuvoa kuljetettaessa. Ajokortti osoittaa luotettavasti vain kortinhaltijan ajo-oikeuden. Sitä ei ole tarkoitettu tai luotu henkilöllisyyttä osoittavaksi asiakirjaksi, eikä myöntöprosessiin sen vuoksi sisälly välttämättä lainkaan tunnistusta. Asiakirjan luotettavuus ei perustu pelkästään sen vaikeaan fyysiseen väärennettävyyteen vaan

myös ja eritoten myöntöprosessin luotettavuuteen. Ajokorttia ei siis tule rinnastaa henkilöllisyyttä osoittaviin asiakirjoihin (passi ja henkilökortti).

Ajokortin turvatekijät ovat huomattavasti heikompia kuin passissa ja henkilökortissa. Lisäksi joissakin maissa kuten Ranskassa ja Belgiassa on edelleen käytössä pahviset ajokortit, joihin on nidottu henkilön kuva. Ajokortista ei myöskään käy ilmi henkilön kansalaisuus, vaan ajokortin myöntävän maan kirjainlyhenne.

Kaiken kaikkiaan vuonna 2009 voimassa olevia ajokortteja oli Liikenteen turvallisuusviraston mukaan 3 541 352 kappaletta.

Ajokorttia käytetään yleisesti tunnistamisasiakirjana asioimistilanteissa, vaikka sitä ei ole alun perin sellaiseksi tarkoitettu. Esimerkiksi pankit ja kaupat hyväksyvät ajokortin tunnistamisasiakirjana. Kauppojen osalta on huomioitava, että sirullisten maksukorttien yleistyessä ajokortin käyttö korvautuu PIN-koodilla.

Jos poliisissa asioidessaan passin tai henkilökortin hakijalla ei ole esittää tunnistamisasiakirjana voimassa olevaa passia tai henkilökorttia, voidaan myös ajokorttia käyttää apuna henkilön tunnistamisessa. Esitetyn ajokortin lisäksi poliisi pyrkii varmistumaan hakijan henkilöllisyydestä muun muassa rekisterikyselyillä ja mahdollisesti haastattelemalla hakijaa. Lähtökohtaisesti passia ja henkilökorttia haettaessa on oltava vanha asiakirja mukana.

3.4.3.1 Ulkomaalaisille vaihdettavat ajokortit

Suomessa poliisin on vaihdettava Geneven ja Wienin tieliikennesopimusvaltioiden kansalaisten ulkomaiset ajokortit suomalaisiin. Sopimusvaltioita on paljon, esimerkiksi Syyria, Haiti, Nigeria, Togo ja Ruanda. Valtio sitoutuu tieliikennesopimuksissa kohtelemaan toista sopimuksen osapuolta vastavuoroisuusperiaatteen mukaisesti. Tästä syystä kotimaisessa ajokorttiasetuksessa on säädetty, että sopimusmaan ajokortti on voimassa Suomessa määräajan ilman ajokortin vaihtamista suomalaiseen ajokorttiin. Lisäksi ajokorttiasetuksessa on säädetty siitä menettelystä, jolla sopimusmaan ajokortin voi vaihtaa suomalaiseen ajokorttiin. Sopimusvaltioiden kansalaiset voivat vaihtaa ajokorttinsa suomalaiseen puolen vuoden maassa oleskelun jälkeen, mikäli haluavat ajaa Suomessa ilman uutta kuljettajatutkintoa. Lisäksi vaihdetaan muiden EU-maiden kansalaisten ajokortteja suomalaisiin.

Ajokorttiin ei ole mahdollista tehdä merkintää varmistamattomasta henkilöllisyydestä, toisin kuin muukalaispassiin tai pakolaisen matkustusasiakirjaan.

Ulkomaisia ajokortteja vaihdetaan suomalaisiin useita tuhansia vuodessa ja määrä kasvaa vuosi vuodelta. Vuoden 2008 vaihtomäärä oli 25 % suurempi kuin edellisenä vuonna.

Taulukko 1: Vaihdetut ulkomaiset ajokortit vuosina 2005–2010. (Lähde: Liikenteen turvallisuusvirasto, 2010.)

Vuosi	***EU & ETA-maat***	***Muut maat***	***Yhteensä***	
2005	991	1997	2988	
2006	907	2304	3211	
2007	1150	2198	3348	
2008	1335	2838	4173	
2009	1585	2986	4571	
2010			2243	*(30.6.2010 mennessä)*

Liikenteen turvallisuusviraston (Trafi) tilastojen mukaan 30.6.2010 voimassa olevia ulkomaisen ajokortin perusteella myönnettyjä suomalaisia ajokortteja on 35 232 kappaletta.

3.4.4 Kela-kortti

Kaikki Suomen sosiaaliturvan piiriin kuuluvat henkilöt saavat kuvattoman Kela-kortin maksutta. Kuvallinen Kela-kortti on maksullinen. Kansaneläkelaitos on lopettanut kuvallisten Kela-korttien myöntämisen 13.10.2008. Kaikki 13.10.2008 päivämäärään mennessä myönnetyt kuvalliset Kela-kortit ovat kuitenkin normaalisti voimassa, ja henkilöt saavat ilmaisen uusintakortin esimerkiksi henkilö- tai sairausvakuutustietojen muuttuessa. Uusintakortteja myönnetään vuoteen 2014 saakka. Kela päätti luopua kuvallisesta Kela-kortista, koska kuvallinen kortti ei ole asiakkaiden etuuksien hoitamisen kannalta välttämätön eikä se ole henkilöllisyyttä osoittava asiakirja. Maksutonta, kuvatonta Kela-korttia muutos ei koske. Vaihtoehto kuvalliselle Kela-kortille on poliisin myöntämä henkilökortti, johon voidaan liittää sairausvakuutustiedot.

Kuvallista Kela-korttia voi käyttää tunnistauduttaessa Kelan toimistoissa, pankeissa ja posteissa. Muut laitokset ja yritykset päättävät itse, hyväksyvätkö he kuvallisen Kela-kortin tunnistamisasiakirjaksi. Esimerkiksi Alkon myymälät eivät korttia hyväksy. Kortti ei myöskään käy tunnistamisasiakirjana ulkomailla.

Jos henkilö muuttaa pysyvästi pois Suomesta, tulee Kela-kortti palauttaa Kelaan. Jos taas henkilö muuttaa pysyvästi ulkomailta Suomeen, henkilön tulee hakea Suomen sosiaaliturvan piiriin pääsyä, minkä jälkeen hän voi saada Kela-kortin. Kela-kortin myöntöprosessin taso on matala, koska korttia ei ole tarkoitettukaan tunnistamisasiakirjaksi, vaan se osoittaa kuulumisen Suomen sosiaaliturvajärjestelmän piiriin. Kela-kortti on käytännössä suurimmalla osalla Suomessa asuvista henkilöistä.

3.5 Tunnistaminen etänä

Liikenne- ja viestintäministeriö on asettanut arjen tietoyhteiskunnan neuvottelukunnan alaisuuteen sähköisen tunnistamisen kehittämisryhmän. Sähköisen tunnistamisen kehittämisryhmä laati syyskuussa 2008 vahvan sähköisen tunnistamisen kansalliset linjaukset, joissa kuvataan sekä yksityisen että julkisen sektorin näkökulmista se toimintaympäristö, jolle vahvan sähköisen tunnistamisen jatkokehittäminen Suomessa perustuu. Sähköisen tunnistamisen kansalliset linjaukset hyväksyttiin lokakuussa 2008 arjen tietoyhteiskunnan neuvottelukunnassa, jossa ovat edustettuina sähköisen tunnistamisen kehittämisen kannalta tärkeimmät yksityisen ja julkisen sektorin toimijat.

Linjauksissa todetaan tarve luoda Suomeen edellytykset toimivien vahvan sähköisen tunnistamisen markkinoiden syntymiselle. Markkinoille tunnusomaista on tunnistusvälineiden yleiskäyttöisyys ja vapaa kilpailu.

Yleisesti katsotaan, että vahva tunnistaminen koostuu jostain, mitä käyttäjä tietää (kuten esimerkiksi käyttäjätunnus), mitä käyttäjä omistaa (kuten esimerkiksi salasanalista tai kertakäyttöisiä tunnuksia generoiva laite, varmenne tai muu väline), tai mitä käyttäjällä on (kuten esimerkiksi sormenjälki). Vähintään kahden näistä vaatimuksista on toteuduttava samanaikaisesti, jotta tunnistustapahtuma täyttää vahvan sähköisen tunnistamisen määritelmän. Tällä hetkellä kuluttajille suunnattuja vahvan sähköisen tunnistamisen palveluita Suomessa tarjoavat pankit ja Väestörekisterikeskus. Vahvoista menetelmistä selvästi käytetyimpiä ovat pankkien tarjoamat pankkitunnisteet. Markkinoilla on tällä hetkellä yli neljä miljoonaa pankkitunnistetta ja noin 260 000 Väestörekisterikeskuksen tarjoamaa kansalaisvarmennetta. Selkeästi suurin osa tunnistustapahtumista tehdään pankkitunnisteilla.

Linjausten mukaan vahvan sähköisen tunnistamisen luotettavuus perustuu käytettyyn menetelmään, palvelumallin turvallisiin ja auditoitaviin prosesseihin ja toteutustapoihin, lainsäädännössä vahvan sähköisen tunnistamisen palveluiden tarjoamiselle asetettaviin perusedellytyksiin, vahvan tunnistamisen palvelua tarjoavien ja sitä käyttävien palveluntarjoajien muodostamaan luottamusverkostoon sekä viranomaisvalvontaan. Näin toteutettu vahva sähköinen tunnistaminen soveltuu lähtökohtaisesti kaikkeen luotettavaan sähköiseen tunnistamiseen niin yksityisellä kuin julkisellakin sektorilla.

Kohdan perusteluissa todetaan, että suomalaisessa järjestelmässä sekä mahdollinen vahvan sähköisen tunnistusvälineiden tai menetelmien luokittelu että luokittelun hyväksi käyttäminen on jätettävä markkinoiden, eli vahvan tunnistamisen palveluita tarjoavien ja käyttävien palveluntarjoajien sekä loppukäyttäjien omaan harkintaan. Lainsäädännön tasolla Suomessa riittää jako heikkoon eli käytännössä sääntelemättömään ja vahvaan sähköiseen tunnistamiseen. Heikon tunnistamisen menetelmistä yleisimpiä ovat erilaiset käyttäjätunnusten ja salasanojen yhdistelmät. Vahvaa sähköistä tunnistamista säännel-

lään lainsäädäntöteitse lailla vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, joka astui voimaan 1.9.2009.

Olemassa ei ole yleistä sääntelyä siitä, missä tapauksissa palvelu edellyttää vahvaa sähköistä tunnistamista. Yksittäisissä laeissa saattaa olla tällaisia säännöksiä, ja vaikuttaa siltä, että tällaisten säännösten määrä on kasvussa. Liikenne- ja viestintäministeriön kaksivuotisen Luottamus ja tietoturva sähköisissä palveluissa eli LUOTI-ohjelman yhteydessä vahvan sähköisen tunnistamisen käyttötilanteiksi katsottiin yleisesti ottaen taloudellisia tai oikeudellisia sitoumuksia ja luottamuksellisten tietojen, kuten henkilötietolain mukaisten arkaluonteisten henkilötietojen tai organisaation salassa pidettävien tietojen käsittelyä edellyttävät sähköiset palvelut. Julkisen sektorin osalta valtiovarainministeriön ohjeessa 12/2006 on todettu, että vahvaa tunnistamista tarvitaan luottamuksellisissa vuorovaikutteisissa asiointipalveluissa sekä tietojärjestelmien välisessä tietojenvaihdossa eli sovellus-sovellus-asioinnissa.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 5 §:ssä todetaan voimassa oleva oikeustila sen suhteen, että tunnistusvälineillä voidaan tehdä oikeustoimia osapuolten niin halutessa, ellei lainsäädännössä ole erityisiä muotovaatimuksia kyseisen oikeustoimen osalta. Suomessa erityisiä muotovaatimuksia vaativat oikeustoimet ovat huomattavassa vähemmistössä. Jo vuonna 2002 valtiovarainministeriön Vahti-ohjeissa todettiin, että valtionhallinnossa tunnistautumisessa voidaan hyväksyä henkilökortilla sijaitseva kansalaisvarmenne sekä pankkitunnisteet.

3.5.1 Laki vahvasta sähköisestä tunnistamisesta ja sähköistä allekirjoituksista

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009) tuli voimaan 1.9.2009 ja se korvasi lain sähköisistä allekirjoituksista (14/2003). Lain tarkoituksena on edistää vahvan sähköisen tunnistamisen palveluiden tarjontaa ja luoda markkinoille perussäännökset palveluiden tarjontaan. Samalla pyritään varmistamaan, että palveluiden tarjonnassa otetaan huomioon tietoturvan ja tietosuojan vaatimukset. Edistämällä sähköisten tunnistuspalveluiden tarjontaa lain tarkoituksena on edistää sähköisiä palveluita ja sähköistä asiointia yleensä sekä niiden tietosuojaa ja tietoturvaa.

Lailla pyritään luomaan toimivat sähköisen tunnistamisen markkinat antamalla alan toimijoille tietyt perussäännöt. Näiden markkinoiden lähtökohtana ovat tunnistusvälineiden yleiskäyttöisyys ja vapaa kilpailu. Sähköinen tunnistaminen toimii pääsääntöisesti palveluntarjoajien muodostamassa luottamusverkostossa. Tietyt perussäännöt ja niiden noudattamisen valvonta antavat toisille palveluntarjoajille tiedon siitä, että kaikki alan toimijat täyttävät tietyn perustason omassa toiminnassaan. Tämä helpottaa olennaisesti luottamusverkostojen kehittymistä edelleen.

Lain tarkoituksena on myös mahdollistaa sähköisten allekirjoitusten käyttö ja niihin liittyvien tuotteiden ja palveluiden tarjonta. Lain sähköistä allekirjoittamista koskevan

osuuden on tarkoitus panna edelleen täytäntöön EU:ssa voimassa oleva sähköisiä allekirjoituksia koskevista yhteisön puitteista annettu direktiivi. Kansallisen lain sähköisiä allekirjoituksia koskevat osuudet ehdotetaan kuitenkin annettavaksi kokonaan uudelleen sen johdosta, että muutettu laki olisi rakenteeltaan varsin sekava.

3.5.1.1 Sähköinen tunnistaminen

Lailla säännellään vahvan sähköisen tunnistamisen palvelujen tarjoamisesta. Laki kohdistuu luonnollisten henkilöiden tunnistamiseen. Luonnolliset henkilöt voivat muualla lainsäädännössä säädettyjen edustamista koskevien säännösten mukaisesti edustaa toista luonnollista henkilöä tai oikeushenkilöä, mutta roolitiedon liittäminen tunnistamiseen ei kuuluisi ehdotetun lain soveltamisalaan. Nämä palvelut ovat toistaiseksi vielä kehitysvaiheessa.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 10 §:n mukaan Suomeen sijoittautuneiden vahvan sähköisen tunnistuspalvelun tarjoajien on tehtävä Viestintävirastolle ilmoitus palveluiden tarjonnasta. Viestintävirasto tarkistaa palveluntarjoajan ja sen tarjoaman palvelun vastaavaan tapaan kuin laatuvarmennepalvelun sähköisen allekirjoittamisen osalta. Pääsääntöisesti valvonta on kuitenkin jälkikäteistä valvontaa lain 5 luvun säännösten mukaisesti.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 17 § sisältää säännökset vahvaa sähköistä tunnistamista koskevasta henkilön ensitunnistamisesta. Pääsääntönä on se, että vahvan sähköisen tunnistuspalvelun tarjoajan on tunnistettava tunnistusvälineen hakija toteamalla henkilöllisyys voimassa olevasta passista tai Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämästä henkilökortista.

Halutessaan vahvan sähköisen tunnistuspalvelun tarjoaja voi käyttää ensitunnistamisessa myös Euroopan talousalueen jäsenvaltion viranomaisen vuoden 1990 syyskuun jälkeen myöntämää voimassa olevaa ajokorttia. Ensitunnistamisen on tapahduttava henkilökohtaisesti, paitsi jos vahvan sähköisen tunnistuspalvelun tarjoajat ovat tehneet keskenään sopimuksen mahdollisuudesta luottaa toistensa tekemään tunnistukseen. Ensitunnistamisen varsinainen ketjuttaminen ei siten ole mahdollista, vaan alkuperäisen ensitunnistamisen tehneen palveluntarjoajan on aina oltava mukana sopimusjärjestelyissä.

Suurimmat teleyritykset DNA, Elisa ja TeliaSonera ovat ryhtyneet tarjoamaan kuluttajille ja palveluntarjoajille mobiilivarmennetta 30.11.2010 lähtien. Mobiilivarmenne on matkapuhelimessa mukana kulkeva sähköinen tunnistusväline. Varmenne liitetään simkorttiin. Nämä varmenteet ovat ensimmäiset kokonaisuudessaan yksityisen sektorin antamat varmenteet.

3.5.1.2 Sähköinen allekirjoitus

Sähköisen allekirjoituksen osalta sääntely vastaa pääosin sähköisistä allekirjoituksista annetun lain sääntelyä, jolla pannaan täytäntöön sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin säännökset. Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 5 §:n 2 momentissa todetaan, että jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä. Lisäksi todetaan, että sähköiseltä allekirjoitukselta ei tule evätä oikeusvaikutuksia yksinomaan sen vuoksi, että se on tehty muulla sähköisen allekirjoittamisen tavalla. Säännös vastaa voimassa olevaa lakia, mutta jälkimmäinen virke on lisätty sähköisiä allekirjoituksia koskevan yhteisön direktiivin 5 artiklan 2 kohtaa mukaillen.

3.5.2 Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista

Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009) tuli voimaan 1.3.2010 ja korvasi väestötietolain (507/1993). Väestörekisterikeskuksen tehtävänä on väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 6 luvun 66 §:n mukaisesti tuottaa, tarjota ja hallinnoida kansalaisvarmenne sekä 67 §:n mukaiset muut varmenteet varmennettuun sähköiseen asiointiin.

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annettuun lakiin sisältyvien, henkilölle myönnettäviä varmenteita koskevien säännösten tarkoituksena on ollut mahdollistaa kansalaisille viranomaisen takaama henkilöllisyys verkossa asiointia varten samalla tavoin kuin perinteisellä tavalla tapahtuvassa asioinnissa on käytetty henkilöllisyyden osoittamiseen viranomaisen antamia asiakirjoja kuten passia ja henkilökorttia. Viranomaisten palveluissa hyväksytään tunnistamisratkaisuina kansalaisvarmenteen lisäksi myös pankkitunnisteet. Väestörekisterikeskuksen myöntämä varmenne on yleiskäyttöinen ja teknisestä alustasta riippumaton, joten varmenne voidaan periaatteessa tallettaa erilaisille korttialustoille tai muuhun tekniseen välineeseen.

Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista laajensi varmennetussa sähköisessä asioinnissa käytettävän sähköisen asiointitunnuksen käyttöalaa nykyisestään siten, että Väestörekisterikeskuksen on mahdollista luovuttaa tunnus myös muiden Suomeen sijoittuneiden varmentajien käyttöön. Tunnusta on näissä tapauksissa mahdollista käyttää varmenteen haltijan yksilöivänä tunnistetietona vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitetussa varmenteessa.

3.5.2.1 Kansalaisvarmenne

Kansalaisvarmenne sijaitsee poliisin myöntämällä henkilökortilla olevalla sirulla. Kansalaisvarmenne on laatuvarmenne, jota haettaessa tunnistamisen suorittaa poliisi. Sähköinen henkilökortti ja siihen perustuva turvallisen verkkoasioinnin mahdollistama henkilön luotettava tunnistaminen on ollut käytössä joulukuusta 1999 lähtien, ensimmäisenä maailmassa kaikille kansalaisille ja pysyvästi maassa asuville ulkomaalaisille tarjottavana yhteiskunnan perusinfrastruktuuripalveluna. Kansalaisvarmenteen käytön odotettua hitaamman yleistymisen on arvioitu johtuvan muun muassa palveluiden määrän vähäisyydestä ja kortinlukijoiden epämukavuudesta. Lisäksi käytännössä Suomessa käytetään hyvin yleisesti pankkitunnisteita tunnistamistapahtumissa.

Elokuun 2010 loppuun mennessä kansalaisvarmenteita oli myönnetty yhteensä 327 300 henkilölle, joista voimassa olevia on 261 800. Sairausvakuutustietonsa oli yhdistänyt henkilökorttiinsa 149 900 henkilöä. Kansalaisvarmenteen on voinut aiemmin saada käyttöönsä myös mobiilipäätelaitteella sekä pankin kortille yhdistettynä, mutta tämä mahdollisuus on sittemmin lopetettu. Kortinhaltijan varmenteisiin on tallennettu ainoastaan henkilötietoina etu- ja sukunimet ja yksilöivä SATU-tunnus (sähköinen asiointitunnus). SATU-tunnus on sisällöltään juokseva sarjanumero, joka ei kerro haltijastaan mitään, toisin kuin henkilötunnus. Kerran henkilölle luotu SATU-tunnus on elinikäinen. Mikäli kortinhaltija on korttihakemusta jättäessään ilmoittanut sähköpostiosoitteensa varmenteeseen laitettavaksi, on se tällöin osa varmenteen tietosisältöä.

> Hallituksen esitys Eduskunnalle laiksi väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 89/2008: Kansalaisvarmenteella tarkoitetaan Väestörekisterikeskuksen luonnolliselle henkilölle myöntämää varmennetta, joka sisältyy henkilökorttilaissa (829/1999) tarkoitettuun henkilökorttiin tai muuhun siihen verrattavaan viranomaisen asiakirjaan tai tekniseen alustaan, ja jota käytetään henkilön todentamista, sähköisen allekirjoituksen tekemistä sekä asiakirjojen ja viestien salausta varten.
> Säännöksessä tarkoitetun asiakirjan ja teknisen alustan käsitettä määriteltäessä voitaisiin ottaa soveltuvin osin huomioon viranomaisen toiminnan julkisuudesta annetun lain 5 §:n 2 momentin säännökset. Muu henkilökorttiin verrattava viranomaisen asiakirja voisi olla esimerkiksi passi, ajokortti tai muu henkilöllisyyden osoittava asiakirja, jos tällaisiin asiakirjoihin jossakin vaiheessa päätetään sisällyttää henkilövarmenne. Tekninen alusta voisi olla esimerkiksi muistitikku tai tunnistetarra.

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 66 § koskee kansalaisvarmenteen hakemista ja myöntämistä ja 67 § muun varmenteen hakemista ja myöntämistä. Varmenteiden eriyttäminen tarkoittaa käytännössä sitä, että kansalaisvarmenteen rekisteröinti jää poliisille ja henkilön varmenteen hakemiseen liittyvä tunnistaminen tehdään fyysisesti poliisin luona. Muiden varmenteiden osalta tunnistaminen tehdään varmentajan valvonnassa ja vastuulla muualla, esimerkiksi yksityisessä yhteistyöyrityksessä tai yhteisössä.

> Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 66 §:n mukaan kansalaisvarmenne voidaan myöntää vain Suomen kansalaiselle sekä kotikuntalain mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle, jonka tiedot on talletettu väestötietojärjestelmään ja jonka henkilöllisyys on voitu luotettavasti todeta.

> Kansalaisvarmennetta koskeva kirjallinen hakemus on jätettävä henkilökohtaisesti poliisilaitokselle, jossa hakija tunnistetaan ja hänen esittämänsä henkilötiedot tarkistetaan hänen suostumuksellaan väestötietojärjestelmästä. Jos henkilökorttiin talletetaan ja merkitään henkilökorttilain 3 a §:ssä tarkoitettuja tietoja, noudatetaan kansalaisvarmenteen hakemisessa henkilökorttilain 6 §:n 2 momentissa säädettyä menettelyä.
>
> Hakemuksen vastaanottajan on noudatettava henkilötietolaissa säädettyjä henkilötietojen käsittelyä sekä vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa asetettuja varmenteen myöntämistä koskevia vaatimuksia.

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 68 §:n mukaan henkilökohtaisen käynnin sijasta kansalaisvarmenteen uusimista koskeva hakemus voidaan tehdä myös sähköisesti ja allekirjoittaa hakijan käytössä olevalla kansalaisvarmenteella ja muun Väestörekisterikeskuksen tuottaman varmenteen uusimista koskeva hakemus hakijan käytössä olevalla vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 30 §:ssä tarkoitetulla varmenteella, jos tällainen palvelu on käytössä. Edellä mainittu väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 68 §:n sääntely tuo uudistuksen nykytilaan nähden mahdollistaen Väestörekisterikeskuksen tuottaman varmenteen uusimisen sähköisesti voimassa olevan laatuvarmenteen avulla.

Valtion varmennetuotantoa ollaan uudistamassa. Valtiovarainministeriön asettama valtion varmennetuotannon uudelleenorganisointi -hankkeen määräaikaa 3.10.2008 - 30.8.2009 jatkettiin vielä 28.9.2009 - 28.2.2010 väliselle ajalle. Hankkeessa määriteltiin vaihtoehtoiset organisointimallit sille, miten valtion varmennetuotanto kokonaisuudessaan voidaan toiminnallisesti tulevaisuudessa järjestää. Hankkeen väliraportti valmistui 5.6.2009 ja siinä esiteltiin kaksi eri vaihtoehtoa varmennepalveluiden uudelleenorganisoinnille. Työryhmän työ on siis tältä osin päättynyt, mutta lopullista ratkaisua ei ole vielä tehty. Kansalaisvarmenteen osalta on päätetty, että ratkaisu tehdään vuoden 2011 aikana. Jatkotyön tarkempi organisointi ei ole vielä tiedossa.

3.5.2.2 Muut Väestörekisterikeskuksen varmenteet

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 61 § säätelee varmennetun sähköisen asioinnin palveluita:

> Väestörekisterikeskuksen tehtävänä on tuottaa, tarjota ja hallinnoida varmennetussa sähköisessä asioinnissa käytettäväksi tarkoitettu kansalaisvarmenne sekä sen käyttöön välittömästi liittyvät varmennehakemisto- ja sulkulistapalvelut. Väestörekisterikeskus voi lisäksi tuottaa varmennetussa sähköisessä asioinnissa käytettäväksi seuraavat palvelut: 1) muun varmenteen kuin kansalaisvarmenteen tarjoaminen ja hallinnointi, 2) varmennetun sähköisen asioinnin osapuolten todentaminen ja asioinnin hallinnointi, 3) sähköisten asiakirjojen ja viestien sähköinen allekirjoittaminen ja salaaminen, 4) sähköisten asiakirjojen ja viestien aitouden, luottamuksellisuuden ja eheyden säilyttäminen ja varmentaminen, 5) varmennetun sähköisen asiointitapahtuman toimijoiden aseman tai roolin varmentaminen, 6) muun varmenteen kuin kansalaisvarmenteen käyttöön liittyvien varmennehakemisto- ja sulkulistapalvelujen tarjoaminen ja hallinnointi, 7) varmennetun aikaleimapalvelun tarjoaminen ja hallinnointi sekä 8) muu vastaava varmennetun sähköisen asioinnin toiminto tai palvelu.

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 67 §:ssä säädetään muun varmenteen hakemisesta ja myöntämisestä.

Väestörekisterikeskus voi myöntää myös sähköisen allekirjoituksen direktiivin vaatimukset täyttävän laatuvarmenteen. Laatuvarmenteella tarkoitetaan varmennetta, joka täyttää laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista vaatimukset ja jonka on myöntänyt 33–38 §:ssä säädetyt vaatimukset täyttävä varmentaja. Kaikki Väestörekisterikeskuksen myöntämät henkilövarmenteet ovat siis laatuvarmenteita.

Laatuvarmenteen tulee sisältää: 1) tieto siitä, että varmenne on laatuvarmenne, 2) tieto varmentajasta ja sen sijoittautumisvaltiosta, 3) allekirjoittajan nimi tai salanimi, josta ilmenee, että se on salanimi, 4) allekirjoituksen todentamistiedot, jotka vastaavat allekirjoittajan hallinnassa olevia allekirjoituksen luomistietoja, 5) laatuvarmenteen voimassaoloaika, 6) laatuvarmenteen yksilöivä tunnus, 7) varmentajan kehittynyt sähköinen allekirjoitus, 8) mahdolliset laatuvarmenteen käyttörajoitukset; sekä 9) allekirjoittajaan liittyvät erityiset tiedot, jos ne ovat tarpeen laatuvarmenteen käyttötarkoituksen kannalta. (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 30 §).

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 5 §:n 2 momentissa todetaan, että jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä. Näin nämä vaatimukset täyttävät sähköiset allekirjoitukset vastaavat suoraan lain nojalla ilman eri näyttöä perinteiseltä allekirjoitukselta vaadittavia ominaisuuksia.

Väestörekisterikeskuksen tuottama muu luonnollisen henkilön varmenne kuin kansalaisvarmenne voidaan myöntää lain väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 67 § mukaisesti vain Suomen kansalaiselle sekä kotikuntalain mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle, jonka tiedot on talletettu väestötietojärjestelmään ja jonka henkilöllisyys on voitu luotettavasti todeta. Väestörekisterikeskuksen tuottama muu luonnollisen henkilön varmenne kuin kansalaisvarmenne voidaan erityisestä ja perustellusta syystä myöntää myös henkilölle, jonka henkilöllisyys on voitu luotettavasti todeta, mutta joka ei täytä muita edellä tarkoitettuja varmenteen myöntämisen edellytyksiä. Tällainen varmenne voi hakijan pyynnöstä sisältyä sähköisessä asioinnissa käytettävään viranomaisen, yrityksen tai yhteisön myöntämään asiakirjaan, korttiin tai tekniseen alustaan. Väestörekisterikeskus voi sopia asiakirjan tai teknisen alustan myöntävän viranomaisen, yrityksen tai yhteisön kanssa, että varmennetta koskeva hakemus voidaan jättää tälle henkilökohtaisesti Väestörekisterikeskukselle edelleen toimitettavaksi. Väestörekisterikeskuksen on tällöin varmistettava, että hakemuksen vastaanottaja noudattaa henkilötietolaissa säädettyjä henkilötietojen käsittelyä sekä sähköisistä allekirjoituksista annetussa laissa asetettuja varmenteen myöntämistä koskevia vaatimuksia.

Hakemuksen vastaanottajan on tunnistettava hakija toteamalla hänen henkilöllisyytensä voimassa olevasta poliisin myöntämästä henkilöllisyyden osoittavasta asiakirjasta ja tarkistamalla varmenteen hakijan suostumuksella hakijan esittämät henkilötiedot väestötietojärjestelmästä. Jos hakijalla ei ole esittää poliisin myöntämää henkilöllisyyden osoittavaa asiakirjaa tai hakijan tunnistamisen varmistamiseksi on olemassa muita erityisiä syitä, hakijan tunnistamisen suorittaa poliisi. Poliisin myöntämistä henkilöllisyyden osoittavista asiakirjoista voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.

Sellaisen varmenteen hakijan, jolle myönnetään varmenne 1 momentin mukaisesti erityisestä ja perustellusta syystä, henkilöllisyys on todettava toimivaltaisen viranomaisen myöntämästä voimassa olevasta henkilöllisyyden osoittavasta asiakirjasta. Jos hakijalla ei ole esittää toimivaltaisen viranomaisen myöntämää henkilöllisyyden osoittavaa asiakirjaa tai hakijan tunnistamisen varmistamiseksi on olemassa muita erityisiä syitä, hakijan tunnistamisen suorittaa toimivaltainen viranomainen.

3.5.3 Muu tunnistaminen ja todentaminen

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista ei koske heikkoa tunnistamista. Heikko tunnistaminen jää siten täysin tämän lain sääntelyn ulkopuolelle. Heikon tunnistamisen menetelmät ovat nykyään yleisimmin käytettyjä tunnistamismenetelmiä. Käytännössä tämä tarkoittaa käyttäjätunnusten ja salasanojen yhdistelmiä. Tällaisia tunnistamismenetelmiä käytetään nykyään ja jatkossa esimerkiksi internetin erilaisilla keskustelupalstoilla. Niihin liittyy huomattavia käyttömukavuuteen ja tietoturvaan liittyviä ongelmia, joten niiden käyttöä ei lailla erityisesti pyritä edistämään. Riippuen siitä kuinka tunnistaminen on tehty, palveluntarjoajalla tällöin joko on tai ei ole tietoa käyttäjän todellisesta henkilöllisyydestä. Niiden hyvänä puolena on maksuttomuus, minkä johdosta ne sopivat sellaisten palveluiden käyttöön, joissa ei ole kyse taloudellisista eduista tai oikeustoimien tekemisestä.

Tässä työryhmän loppuraportissa keskitytään vahvaan tunnistamiseen.

3.6 Identiteettivarkaudet

Identiteettivarkaus on yleiskielessä käytetty käsite laajalle joukolle erilaisia tekokokonaisuuksia, joille on kuitenkin yhteistä se, että jotakin identiteettitietoa kerätään oikeudetta. Kerättyä tietoa käytetään edelleen oikeudetta joko rikoshyödyn hankkimiseksi tai tavalla, josta aiheutuu identiteetin haltijalle vahinkoa. Identiteettivarkaus on nimityksenä jossain määrin harhaanjohtava, sillä toisin kuin varkausrikoksessa (RL 28:1), identiteettivarkaudessa identiteettiä ei välttämättä oteta missään vaiheessa pois rikosuhrin hallusta. Rikoksentekijä vain kopioi tiedon myös omaan käyttöönsä.

Henkilöllisyysvarkaus on identiteettivarkauden osajoukko, jossa teko kohdistuu nimenomaan henkilöön ja jossa kerättävä tieto on henkilötieto. Tietoverkossa ”identiteetti” voi kuitenkin olla henkilötiedon lisäksi mikä tahansa tunniste, jota käytetään joko vain erottelemaan kokonaisuudet toisistaan tai osoittamaan, että 1) tunnisteen haltija on se, joksi hän itseään väittää tai että 2) tunnisteen haltijalla on oikeus päästä käsiksi tietoon tai palveluun, johon identiteetin todellisella haltijallakin on oikeus.

Identiteettivarkauksilla aiheutetusta vahingosta ei ole saatavilla yhteismitallista tilastotietoa. Esimerkiksi Yhdysvalloissa on laskettu tutkimuksesta riippuen jo vuonna 2006 olleen 8,3 - 15 miljoonaa identiteettivarkauden uhria vuodessa. Britannian pankkiyhdistyksen APACSin julkisen arvion mukaan vuonna 2007 identiteettirikoksiin liittyvissä verkkopankkirikoksissa rikolliset hankkivat rikoshyötyä 29 M€ edestä (arvioituna kesän 2008 euro-punta-kurssilla) kun samaan aikaan Suomessa vastaava summa oli hiukan yli 50 000 €. EU:ssa toimivan väärät asiakirjat -työryhmän kartoituksen mukaan (12/2008) 70 % EU-maista ilmoitti, että heillä on havaittu henkilöllisyysvarkauksia.

Suomessa poliisin tilastointi perustuu lähtökohtaisesti rikosnimikkeisiin. Koska identiteettivarkauden kuvaavaa rikosnimikettä ei ole, tilastoja ei ole automaattisesti saatavilla, vaan identiteettivarkauksiin liittyvät tapaukset tulisi seuloa käsin koko rikosilmoitusmassasta. Tehtävä on mittava, sillä identiteettivarkaus saattaa ilmetä myös petosrikoksena tai kunnianloukkauksena, joita kirjataan vuosittain valtavat määrät myös muunlaisilla tekotavoilla.

3.6.1 Identiteettivarkauksia sivuava muu aikaisempi tarkastelu

Sekä EU:n tasolla että useissa jäsenmaissa, myös Suomessa pohditaan juuri nyt identiteettivarkauksien kriminalisoinnin tarvetta, sillä tietoverkko on muuttanut toimintaympäristöä merkittävästi.

3.6.1.1 Väärillä henkilötiedoilla esiintyminen

Ennen vuotta 1999 rikoslain 42 luvun 5 §:ssä todettiin: On rangaistava sakolla sitä, joka erehdyttääkseen yksityistä henkilöä käytti toisen passia, työtodistusta tai muuta sen kaltaista todistusta. Säännös kuitenkin kumottiin, koska pykälässä kuvattu epärehellisyys liittyi käytännössä yleensä jonkin muun rikoksen tekemiseen. Pykälän tultua kumotuksi pelkkä muulla kuin omalla nimellä esiintyminen tai väärän iän ilmoittaminen muulle kuin viranomaiselle ei ole rangaistavaa.

Lähes samansisältöistä pykälää ehdotettiin palautettavaksi takaisin rikoslain uudistuksessa 2006, mutta lakivaliokunta (LaVM 15/2005) katsoi tuolloin, ettei kriminalisoinnille ollut riittäviä perusteita ja poisti pykälän. Teolla olisi pyrittävä oikeudellisesti merkityksellisen tiedon antamiseen. Rangaistussäännös olisi käytännössä tullut kohdistumaan yksinomaan alaikäisiin.

> Vuonna 2005 ehdotettu ja hylätty rikoslain 5 a §. Toiselle kuuluvan henkilötiedon väärinkäyttö: Joka erehdyttääkseen yksityistä henkilöä antaa oikeudellisesti merkityksellisen tiedon käyttämällä toisen henkilön henkilöllisyyttä, henkilötodistusta, passia, ajokorttia tai muuta sen kaltaista viranomaisen myöntämää todistusta, on tuomittava toiselle kuuluvan henkilötiedon väärinkäytöstä sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.

Lakivaliokunta katsoi, että tunnusmerkistö täyttyisi jo pelkästään toisen henkilötodistuksen käyttämisellä ilman, että tällaisella käyttämisellä tavoiteltaisiin taloudellista hyötyä - jolloin kyseeseen voisi tulla petosrikos - tai että henkilötodistusta olisi millään tavoin muunneltu, jolloin kyseessä saattaisi olla väärennysrikos.

Hallituksen esitys eduskunnalle laiksi rikoslain muuttamisesta ja eräiksi siihen liittyviksi laeiksi (169/2005) mukaan toisen henkilötodistuksen tai vastaavan asiakirjan käyttäminen yksityisen henkilön erehdyttämiseksi täyttää rikoslain 36 luvun 1 §:n 1 momentissa rangaistavaksi säädetyn petoksen tunnusmerkistön vain, jos kaikki pykälässä säädetyt rangaistavuuden edellytykset täyttyvät.

> Petos (RL 36:1) Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä, on tuomittava petoksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Hallituksen esityksessä (169/2005) todetaan, että ehdotettua kriminalisointia voidaan kuitenkin pitää tärkeänä keinona osoittaa paheksuntaa viranomaisen myöntämän asiakirjan väärinkäytöstä erehdyttämistarkoituksessa. Ensisijaisena keinona nuorten suojaamista koskevien säännösten ja määräysten noudattamisessa on tehokas valvonta. Kriminalisoinnilla on kuitenkin tärkeä valvontaa tukeva merkitys.

Lakivaliokunta siis (LaVM 15/2005) katsoi, ettei kriminalisoinnille ollut yhteiskunnallista tarvetta. Lakivaliokunta ei kuitenkaan sulkenut pois mahdollisuutta puuttua säännöksessä tarkoitetun kaltaiseen käyttäytymiseen myös rikosoikeudellisin keinoin, jos hallitus myöhemmin esittää tarkoin kohdennettua tunnusmerkistöä, jonka säätämiselle on osoitettavissa asianmukaisiin selvityksiin pohjautuva painava yhteiskunnallinen tarve ja joka muutoinkin täyttää valiokunnan käytännössään uudelle rikossäännökselle asettamat vaatimukset.

3.6.1.2 Valtioneuvoston periaatepäätös sähköisestä tunnistamisesta

Hallitus hyväksyi periaatepäätöksen sähköisestä tunnistamisesta 5.3.2009. Kyse on sarjasta toimia, jotka kuuluvat useiden eri ministeriöiden toimivaltaan. Keskeistä on, että ministeriöt ovat mukana toistensa hankkeissa sekä ovat tietoisia aikaisemmista ja käynnissä olevista hankkeista.

> Valtioneuvoston periaatepäätös sähköisestä tunnistamisesta 6 kohta: Henkilön yksilöivien tietojen anastaminen ja väärän henkilöllisyyden käyttäminen

Toisen henkilöllisyyden väärinkäytön erilaiset muodot ovat nopeasti yleistyvä rikollisuuden muoto ja kansainvälisesti vakava ongelma. Toisen henkilöllisyyden väärinkäyttö liittyy usein järjestäytyneeseen rikollisuuteen tai laittomaan maahanmuuttoon. Vääriä identiteettejä käytetään usein taloudellisiin etuihin liittyvissä rikoksissa. Useat maat ovatkin ryhtyneet mittaviin toimenpiteisiin estääkseen tämän kaltaiset rikokset. Henkilöllisyyttä suojataan lainsäädännössä välillisesti usein eri säännöksin, mutta sääntely ei ole välttämättä täysin kattavaa. Lainsäädäntöä saatetaan tarvita tilanteissa, jossa tietoverkkorikollisuuteen liittyy väärän henkilöllisyyden käyttö. Lainsäädännön kartoittamisen ohessa on syytä tarkastella myös terminologiaa ja sen yhteneväisyyttä

Verkkorikollisuus on mitä suurimmassa määrin piilorikollisuutta. Käytännössä yleensä toisen henkilön yksityisiä tietoja, kuten luottokortin numeroa, käytetään luvatta muiden rikosten tekemiseen. Useissa muissa EU:n jäsenvaltioissa väärän henkilöllisyyden käyttö rangaistaan usein petoksena tai se ei ole rangaistavaa lainkaan. Yhtäläinen lainsäädäntö jäsenmaissa voisi helpottaa lainvalvontaviranomaisten välistä yhteistyötä. Komissio on aloittanut kuulemisen siitä, onko yhtäläinen lainsäädäntö tältä osin tarpeen.

Kansalaisen itsensä ei voi olettaa olevan tietoturvallisuuden asiantuntija, joten hänelle tarjottavan tunnistautumis- tai allekirjoitusmenetelmän tulisi olla ehdottoman luotettava. Kansalaisen oikeusturvan kannalta oman henkilöllisyyden suojaaminen on hyvin keskeistä. Henkilöllisyyden suojaamista voidaan pitää kansalaisen perustavaa laatua olevana oikeutena.

Tavoitteet:
Henkilön yksilöivien tietojen anastaminen ja väärän henkilöllisyyden käyttäminen on voitava estää tehokkaasti. Mahdollisen lainsäädännön lisäksi tarvitaan tehokasta koulutusta ja tiedottamista.

Valtioneuvoston hyväksymän ja sisäasiainministeriön johtaman sisäisen turvallisuuden ohjelman yksi osa-alue on tietoverkkorikollisuus ja siihen liittyvät identiteettivarkaudet. Sisäasiainministeriön henkilöllisyyden luomista koskevan hankkeen (jäljempänä Identiteettiohjelma) yksi keskeisistä tavoitteista on henkilöllisyyden turvaaminen ja toisen henkilöllisyyden väärinkäytön ennalta estäminen. Poliisilla on toisen henkilöllisyyden väärinkäytön osalta keskeinen käytännön toimijan rooli.

Keinot:
Sisäisen turvallisuuden ohjelmassa ja identiteettiohjelmassa tarkastellaan henkilön yksilöivien tietojen anastamista ja väärän henkilöllisyyden käyttämistä ilmiönä. Hankkeissa selvitetään muun muassa, millaisista ilmenemismuodoista voi olla kysymys ja mikä on niiden aiheuttama uhka kansalaisille nyt ja tulevaisuudessa. Lisäksi selvitetään, miltä osin nykyinen lainsäädäntö, erityisesti rikoslaki, vastaa tähän ongelmakenttään, ja onko tarvetta lisäsääntelylle. Ohjelmissa ovat edustettuina useat ministeriöt, muun muassa liikenne- ja viestintäministeriö, oikeusministeriö ja valtiovarainministeriö.

Valtioneuvoston periaatepäätöstä sähköisestä tunnistamisesta valmisteltaessa on käyty ministeriöiden (LVM, VM, SM ja OM) välistä keskustelua identiteettivarkauksien kriminalisoimisen tarpeesta.

Oikeusministeriö on lausunut periaatepäätöksen valmisteluvaiheessa muun muassa seuraavaa: Toisen henkilötietojen väärinkäyttö on jo nyt rangaistavaa teon luonteesta riippuen petoksena, maksuvälinepetoksena, väärennyksenä, henkilörekisteririkoksena, rekisterimerkintärikoksena, väärän todistuksen antamisena viranomaiselle, väärän henkilötiedon antamisena, vahingontekona, luvattomana käyttönä, tietojärjestelmän häirintänä jne. Lisäksi jo maksuvälinepetoksen valmistelu on säädetty erikseen rangaistavaksi (RL 37:11).

Ongelmaksi voi muodostua henkilötietojen väärinkäyttö, jota ei tehdä taloudellisen edun tavoittelun takia, vaan pelkästään kiusanteko, pilailu, tai ei mitään -mielessä. Toisen henkilötietojen käyttöön sellaisenaan, ilman taloudellisen hyödyn tarkoitusta tai vahingoittamistarkoitusta, on vain rajoitetusti katsottu olevan tarvetta puuttua rikosoikeudellisin keinoin. Tällainen henkilötietojen käyttäminen voi olla esim. henkilörekisteririkos tai väärän henkilötiedon antaminen. Esimerkiksi vuonna 2005 lakivaliokunta (LaVM 15/2005) torjui hallituksen esityksen, joka koski henkilön erehdyttämistä henkilötodistusta, passia, ajokorttia tai muuta sen kaltaista henkilötodistusta käyttämällä. Lakivaliokunta katsoi, että ehdotettu tunnusmerkistä täyttyisi jo pelkästään toisen henkilötodistuksen käyttämisellä ilman, että tällaisella käyttämisellä tavoiteltaisiin taloudellista hyötyä - jolloin kyseeseen voisi tulla petosrikos - tai että henkilötodistusta olisi millään tavoin muunneltu, jolloin kyseessä saattaisi olla väärennysrikos. Lakivaliokunnan mielestä tällainen käyttäytyminen ei ole sillä tavoin moitittavaa, että siihen tulisi reagoida rikoslain avulla.

Toisen henkilön tietojen pelkän ”luvattoman” haltuun ottamisen kriminalisointi ei ole tarkoituksenmukaista eikä järkevällä tavalla mahdollistakaan ottaen huomioon, kuinka laajoja ovat mahdollisuudet saada toisen henkilötietoja laillisesti. Toisen henkilön tietoja saa haltuunsa esimerkiksi kysymällä, tiedotusvälineistä, julkisista rekistereistä ja internetistä. Henkilötiedon käsite on varsin laaja (esim: henkilötiedolla tarkoitetaan henkilötietolain 22.4.1999/523 mukaan ”kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi). Tällaisia tietoja on jokaisella jostakin toisesta henkilöstä. Vaikka rajoituttaisiinkin vain henkilötunnukseen, joka on eräs kriittisimmistä vahingollisen käyttömahdollisuuden kannalta, niitä on saatavissa varsin helposti myös laillisesti.

Perustuslain 8 §:ssä ja useissa Suomea sitovissa kansainvälisissä ihmisoikeussopimuksissa säädetty rikosoikeudellinen laillisuuspariaate estäisi säätämästä rangaistavaksi esimerkiksi yleisesti henkilötiedon keräämisen tai käytön, joka on omiaan aiheuttamaan vahinkoa. Tällaisen yleisluontoisen rangaistussäännöksen ongelmana olisi, että se kattaisi rajoittamattoman määrän tekoja ja siten myös sellaista henkilötiedon keräämistä tai käyttämistä, jolla voi olla yhtä hyvin olla hyväksyttävä tai ainakin haitaton tarkoitus. Laillisuusperiaate edellyttää rangaistavan teon määrittelyä täsmällisesti ja tarkkarajaisesti.

Toisen suojaamattoman henkilötiedon haltuun ottamiseenkaan ei ole perusteita puuttua rikosoikeudellisin keinoin ja suojattujen henkilötietojen haltuunotto on jo nykyisin rangaistavaa. Näin ollen oikeusministeriö katsoo, ettei ole tarpeen kriminalisoida myöskään toisen henkilötietojen haltuun ottoa.

Lisäksi tarkastelussa on otettava huomioon yleiset kriminalisointiperusteet, joita on muotoiltu Eduskunnan perustuslakivaliokunnan käytännössä (PeVL 23/1997). Periaatteiden mukaan muun muassa (1) rikosoikeutta tulee käyttää vain tärkeiksi katsottavien etujen suojaamiseksi, (2) rikosoikeuden tulee olla viimesijainen keino (ns. ultima ratio -periaate), (3) kriminalisoinnista tulee olla enemmän hyötyä kuin haittaa ja (4) kriminalisoinnin tulee olla toimiva ja täytäntöönpantavissa myös käytännössä.

3.6.1.3 Neuvoston puitepäätös 2005/222/YOS tietojärjestelmiin kohdistuvista hyökkäyksistä

Neuvoston puitepäätöksen 2005/222/YOS tietojärjestelmin kohdistuvista hyökkäyksistä (24.2.2005) tavoitteena on parantaa oikeus- ja muiden toimivaltaisten viranomaisten, jäsenvaltioiden poliisi- ja muut erikoistuneet lainvalvontaviranomaiset mukaan luettuina, yhteistyötä lähentämällä jäsenvaltioiden rikosoikeudellisia säännöksiä, jotka koskevat tietojärjestelmiin kohdistuvia hyökkäyksiä.

3.6.1.4 Komission tiedonanto neuvostolle, Euroopan parlamentille ja alueiden komitealle - Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi

Tietoverkkorikollisuuden osalta EU:ssa on jo vuonna 2007 aloitettu kuuleminen aiheesta, tarvitaanko lainsäädäntöä tilanteessa, jossa tietoverkkorikollisuuteen liittyy väärän henkilöllisyyden käyttö. Tällä tarkoitetaan usein sitä, että toisen henkilön yksityisiä tietoja, kuten luottokortin numeroa, käytetään luvatta muiden rikosten tekemiseen. Useimmissa jäsenvaltioissa rikollinen asetettaisiin tällaisessa tapauksessa todennäköisesti syytteeseen petoksesta tai jostakin muusta rikoksesta eikä väärän henkilöllisyyden käytöstä, sillä edellistä pidetään vakavampana rikoksena. Väärän henkilöllisyyden käyttöä ei ole määritelty rikokseksi kaikissa jäsenvaltioissa. Asiakirjassa todetaan, että usein on kuitenkin helpompi näyttää toteen väärän henkilöllisyyden käyttö kuin petos, joten EU:n lainvalvontayhteistyön kannalta olisi parempi, jos väärän henkilöllisyyden käyttö määriteltäisiin rikokseksi kaikissa jäsenvaltioissa.

3.6.1.5 Komission kuulemistilaisuudet identiteettivarkauksista Brysselissä

Komissio järjesti Brysselissä 23 -24.11.2009 identiteettivarkauksista kuulemistilaisuuden. Komissio on ottanut identiteettivarkauden erityistarkasteluun, koska entistä enemmän identiteettitiedon kaappaus johtaa petoksiin, maksuvälinepetoksiin, laittoman maahantulon järjestämiseen, rahanpesuun sekä jopa terrorismin rahoittamiseen. Komissio näki keskeisinä kysymyksinä uhrin aseman suojaamisen sekä rikostorjunnan edellytysten turvaamisen. Komissio näkisi hyödyllisenä, jos jäsenmaissa olisi yksi yhteinen määritelmä identiteettivarkauksille. Tällä hetkellä identiteettivarkaus on vain muutamassa jäsenmaassa kriminalisoitu sellaisenaan, mutta tiedon käyttäminen väärin täyttää useimmissa maissa jonkin rikostunnusmerkistön. Komissio koordinoi jäsenmaihin kohdistunutta lainsäädäntöselvitystä, joka valmistui syksyllä 2010.

Komissio järjesti Brysselissä 4-5.10.2010 toisen asiantuntijakokouksen identiteettivarkauksista. Kokouksessa esiteltiin johtopäätelmiä selvityksestä, jossa oli käyty läpi identiteettivarkauksiin ja -petoksiin liittyviä säännöksiä 34 maan (myös EU:n ulkopuolisia maita) lainsäädännössä. Yksi keskeisimmistä havainnoista ehkä oli, että aiheeseen liittyvä käsitteistö kaipaisi koordinointia ainakin EU -maiden kesken. Tutkimuksen johtopäätös oli, ettei kansallisissa rikoslaeissa ole merkittäviä aukkoja, vaikka vain harvassa jäsenvalioissa on erityinen identiteettivarkautta koskeva rangaistussäännös. Seuraamuksissa sekä ehkäisy- ja raportointikeinoissa on sen sijaan eroja.

EU-tasolla on käynnissä myös ASINP -projekti (Strenghtening Architectures for the Identification of Natural Persons in Europe). ASINP -projektiin on tarkoitus sisällyttää kaikki identiteettiketjun 'lenkit' eli id -petokset, dokumenttien väärentämisen helppous/vaikeuttaminen, biometriikka, dokumenttien sisältökysymykset sekä eri maiden lainsäädännön ja hallinnon suhtautuminen ID -petoskysymyksiin.

3.6.2 Perinteiset identiteettivarkaudet

Perinteisillä identiteettivarkausteoilla tarkoitetaan tässä yhteydessä perinteisillä asiakirjoilla (passi, henkilökortti, ajokortti jne.) reaalimaailmassa tehtäviä tekoja. Tyypillisesti perinteiset identiteettivarkaudet tuleva ilmi väärennysrikoksina (RL 33) tai petosrikoksina (RL 36).

Rikoslaissa on eräitä pykäliä, jotka suojaavat henkilöllisyyttä joko suoraan tai välillisesti. Toisena henkilönä esiintyminen viranomaiselle on rikoslain 16 luvussa kattavasti kriminalisoitu: Väärän henkilötiedon antaminen viranomaiselle (RL 16:5), rekisterimerkintärikos (RL 16:7) sekä väärän todistuksen antaminen viranomaiselle (RL 16:8).

Sen sijaan yksityiselle toisena henkilönä esiintymistä ei ole sellaisenaan kriminalisoitu. Rikoslain 16 luvun 5 §:n perusteluissa (HE 6/1997 vp, s.67) nimenomaisesti todetaan, että väärän nimen ilmoittaminen tai muun sellaisen väärän tiedon antaminen yksityishenkilölle ei ollut ehdotetun lainkohdan mukaan rangaistavaa. Sama koskee väärän henkilötiedon antamista pankissa, vakuutusyhtiössä, kaupassa tai muussa vastaavassa paikassa lukuun ottamatta sellaisia poikkeuksellisia tapauksia, joissa kyseinen liikeyritys toimii julkista valtaa käyttävän viranomaisen apuna. Rangaistavuuden edellytyksenä on, että henkilö on tietoinen antamiensa tietojen menemisestä viranomaiselle (KKO 1995:31). Perustelujen mukaan väärän henkilötiedon antamisesta rikoslain 16 luvun 5 §:n tarkoittamassa mielessä ei ole kyse, jos virkamies ei kyseisessä yhteydessä toimi viranomaisena, vaan esimerkiksi erilaisten tavaroiden tai palveluiden tuottajana. Jos kuitenkin toisena esiintymisen tarkoituksena on taloudellisen edun tavoittelu, voi petosrikoksen (RL 36 luku) tunnusmerkistö täyttyä tai, jos tavoitteena on maineen pilaaminen, kyseeseen voi tulla kunnianloukkaus (RL 24).

Perustuslakivaliokunta on katsonut lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista valiokuntakäsittelyssä (PeVL 16/2009), ettei muiden laatuvarmenteiden kuin kansalaisvarmenteen tarjoamista ole enää nykyisin pidettävä julkisena hallintotehtävänä (tarkemmin luvussa 3.3.2 Julkisen vallan käyttö, s. 28). Oikean, mutta varastetun asiakirjan esittäminen yksityiselle palveluntarjoajalle esimerkiksi sähköisen varmenteen hankkimiseksi tai muutoin ei ole siis nykyisellään jo itsessään rangaistavaa.

3.6.3 Tietoverkoissa toteutettavat identiteettivarkaudet

Tietoverkko on muuttanut identiteettitiedon väärinkäyttöä olennaisesti. Tietoverkossa toteutetun rikollisuuden erityisenä ominaispiirteenä on suuri hyötypotentiaali suhteessa pieniin toteutuskustannuksiin sekä kiinnijäännin riskiin. Reaalimaailmassa identiteettivarkaudet ovat usein yksittäistapauksia, mutta verkossa toiminnan voi automatisoida, jolloin rikoksentekijät voivat käsitellä kohtuullisen pienin kustannuksin jopa miljoonittain oikeudetta hankittuja identiteettejä. Kiinnijäännin riski on verkossa reaalimaailmaa pienempi, koska rikokset tehdään jälkien peittämiseksi sivullisilta rikollisten haltuun

kaapatuista verkkoliittymistä, jolloin tutkintatoimet kohdistuvat aina ensin sivulliseen. Rikoksentekijän näkökulmasta verkko on myös täysin globaali. Kukin viranomainen taas on toimivaltainen vain omassa oikeuspiirissään.

Jäljempänä tarkastellaan erikseen taloudellista hyötyä tavoittelevia tekoja, uhria vahingoittamaan pyrkiviä tekoja, sekä sellaisia tekoja, joiden ensisijaisena tavoitteena ei ole kumpikaan edellisistä, mutta jotka aiheuttavat silti haittaa teon kohteelle.

3.6.3.1 Taloudellista hyötyä tietoverkoissa tavoitteleva identiteettirikollisuus

Ammattimaisesti ja järjestäytyneellä tavalla tietoverkossa toimivien rikoksentekijöiden tavoitteena on yksinkertaisesti taloudellinen hyöty mahdollisimman pienellä riskillä. Rikoshyötyä pyritään hankkimaan kaappaamalla rikoksen uhreilta mitä tahansa automatisoidusti kerättävissä olevaa ja helposti rahaksi muutettavaa tietoa, joka lähes aina on jonkinlaista identiteettitietoa. Kohteena ovat tyypillisesti maksuvälinetunnisteet, kuten esimerkiksi luottokorttinumerot, verkkopalveluiden asiointitunnukset sekä sähköpostiosoitteet. Entistä enemmän rikolliset keräävät kuitenkin myös muuta henkilötietoa, kuten henkilöiden nimiä, katuosoitetietoja, henkilötunnuksia ja työnantajatietoja. Tietoa käytetään törkeiden petosten, törkeiden maksuvälinepetosten sekä niihin liittyvän törkeän rahanpesun lisäksi laittoman maahantulon järjestämiseen. EU-alueella on myös konkreettista näyttöä tietojen käyttämisestä terrorismin rahoittamiseen.

Verkon identiteettirikosten ansaintalogiikka perustuu ennen kaikkea tietomassan valtavaan kokoon. Vaikka yksittäinen luottokorttinumero ei vielä kovin arvokas olekaan, miljoona luottokorttinumeroa muodostaa merkittävän resurssin, jota käytetään esimerkiksi kalliin elektroniikan sekä muun helposti jälleenmyytävän omaisuuden hankkimiseen verkkokaupoista. Ansaintalogiikka ei siten perustu ensisijaisesti jonkin todella arvokkaan yksittäisen tiedon – kuten yrityssalaisuuden – kaappaamiseen, vaan kyse on nimenomaan massailmiöstä. Todella arvokkaan tiedon saaminen käsiin on sattumanvaraista. Sen suunnitelmallinen hankkiminen kohdistetulla hyökkäyksellä on olennaisesti kalliimpaa ja hankalampaa. Sen sijaan satunnaisesti valikoidun määrämuotoisen identiteettitiedon hankkiminen onnistuu varmasti ja kohtuullisilla kustannuksilla.

Rikollinen pyrkii iskemään ensisijaisesti sinne, missä tieto on helpoiten saatavilla. Onnistuneen tietokaappauksen edellytyksenä on lähes aina jokin erityinen haavoittuvuus tiedon käsittelyn prosessissa.

Suurimmat yksittäisellä teolla toteutetut luottokorttidataan kohdistuvat tietokaappaukset ovat tapahtuneet palvelimista, jossa tietoja on käsitelty luottokorttiyhtiöiden sopimusehtojen vastaisesti puutteellisesti suojattuna.

> Näyttävänä esimerkkinä tästä on yhdysvaltalaisen maksunvälittäjän, Heartland Payment Systemsin murto vuoden 2007 lopussa, jolloin rikollisten käsiin päätyi 130 miljoonaa luottokorttinumeroa. Eräs tuore Suomea sivunnut esimerkki on Espanjassa tapahtunut

tietomurto, jonka yhteydessä yli 100 000 suomalaista luottokorttinumeroa joutui rikollisten käsiin. Tiedon kaappausta ei sinänsä ole kriminalisoitu, mutta sen toteutuminen edellyttää yleensä valmistelevana toimena tietomurtoa (RL 38:8)) tai luvatonta käyttöä (RL 28:7).

Koska palvelinten suojaus on luottokorttien käsittelyyn liittyvien siviilioikeudellisten vastuukysymysten takia parantunut, tietokaappauksia tehdään enenevässä määrin asiakaspään työasemista ja mobiililaitteista, joista voi kaikkein todennäköisimmin löytää puutteellisesti suojattuja kohteita jatkossakin. Massakeruuta voidaan toteuttaa asiakaspäässä hyvin erilaisilla menetelmillä.

Tietoa voidaan klassisesti huijata käyttäjältä:

Phishingiksi kutsutaan tiedonhankintamenetelmää, jossa tietoa kysytään suoraan käyttäjältä kohtalaisen järkevältä kuulostavalla peitetarinalla. Tällöin rikoksentekijä väärentää esimerkiksi verkkokaupan nimissä sähköpostiviestin, jossa valittelee asiakasrekisteriongelmaa ja pyytää käyttäjää päivittämään asiakastietonsa WWW-lomakkeella. Lomake ei kuitenkaan talleta tietoja verkkokaupan vaan rikoksentekijän hallussa olevaan tietovarastoon. Teko täyttää yleensä petoksen (RL 36:1) tunnusmerkistön.

Koska suuri osa käyttäjistä ei enää usko huijaussähköposteihin, rikolliset ovat kehittäneet tietoteknisiä menetelmiä kaapata tietoja myös asiakaspäästä:

1. Liikenteen uudelleenohjaus: Käyttäjän huijaamisen lisäksi käyttäjä voidaan ohjata virheelliseen osoitteeseen myös puuttumalla haavoittuvan työaseman liikenteenohjaukseen tietoteknisin keinoin. Tällöin rikolliset murtautuvat käyttäjän työasemalle ja muuttavat niin sanottuja nimipalveluasetuksia siten, että käyttäjän avatessa yhteyden verkkokauppaan, yhteys kirjautuukin rikollisen hallussa olevaan palveluun, jolloin rikollinen saa kerättyä käyttäjän ”verkkokauppaan” antamat kirjautumistunnukset.
2. Näppäinpainallusten nauhoitus: Käyttäjän koneelle syötetään päivittämättömän WWW-selaimen, sähköpostiohjelman tai jonkin edellisten käyttämän apuohjelman haavoittuvuutta hyväksikäyttäen haittaohjelma. Haittaohjelma voi kerätä WWW-lomakkeiden näppäinpainalluksia (a keylogger), jolloin rikoksentekijä voi saada haltuunsa esimerkiksi luottokorttinumeron tarkistetietoineen, jos käyttäjä maksaa sillä ostoksiaan verkkokaupassa.
3. Asiointiyhteyksien kaappaus: Näppäinpainallusten nauhoitus ja pankkitunnusten hyväksikäyttö on ollut maailmalla suosittu menetelmä pankkitilien tyhjentämiseen verkkopankkien kautta. Suomessa menetelmä ei ole koskaan toiminut, sillä Suomessa toimivilla pankeilla tietoturvallisuus on aina ollut verkkopankkijärjestelmän suunnittelukriteeri. Kun muualla tietoturvallisuus on parantunut, rikolliset ovat kehittäneet yhteydenkaappausmenetelmiä, joilta kaksivaiheinen tunnistuskaan ei suojaa. Menetelmät ovat kuitenkin aiempaa monimutkaisempia ja niiden hyödyntäminen vaatii tarkkaa räätälöintiä kohdejärjestelmään. Osa teknisistä tiedonhankintamenetelmistä täyttää petoksen (RL 36:1) tunnusmerkistön, osaa edeltää vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9a), kuitenkin irrallisena tekona. Osaa lainsäätäjä ei nykyisellään pidä moitittavana.

Tietoverkossa toteutetuilla tietorikoksilla hankitaan valtaisaa rikoshyötyä – sekä vastaavasti aiheutetaan suurta vahinkoa. Varsin konkreettisesta vahingonuhasta huolimatta esitutkintaviranomaisella ei ole oikeutta tutkia uusilla asiakaspäähän kohdistetuilla tekotavoilla toteutettuja tietokaappauksia eikä siten myöskään estää rikosvahinkoa ennalta, sillä tekotapa ei täytä mitään sellaista rikostunnusmerkistöä, joka mahdollistaisi verkossa välttämättömien teletoimivaltuuksien käyttämisen.

Tutkinta on kyllä osittain mahdollista siinä vaiheessa, kun kaapattuja tietoja käytetään hyväksi törkeän maksuvälinepetoksen tai törkeän petoksen toteuttamiseksi, mutta silloin tiedonkaappausvaiheessa syntynyttä tietoteknistä jälkeä ei enää ole olemassa. Silloin, kun jälki olisi olemassa, esitutkintaviranomainen ei voi sitä hankkia tietoonsa, sillä telepakkokeinojen edellytykset eivät vielä täyty.

Esitutkintaviranomainen ei voi selvittää tietoa kaappaavan haittaohjelmaliikenteen sisältöä, vaikka haittaohjelmaliikennettä onkin vaikea nähdä perustuslain tasoista suojaa nauttivana luottamuksellisena viestintänä. Lainsäädäntö sallii sähköisen viestinnän sisällön selvittämisen tutkittaessa törkeää rahanpesua (RL 32:7), jota käytetään tällaisissa rikoskokonaisuuksissa kaapatun identiteettitiedon muuttamiseen rahaksi. Törkeän rahanpesurikoksen täyttyessä alkuperäistä tietoliikennettä ei kuitenkaan ole enää saatavilla. Telekuuntelua ei myöskään voi kohdistaa alkurikokseen osallistuneisiin tekijöihin, sillä alkurikokseen syyllistyneiden osalta törkeä rahanpesurikos ei täyty (rajausnormi RL 32:11). Toisin kuin suuressa osassa muuta maailmaa, Suomessa niin sanottua ”itsepesua” ei ole säädetty rangaistavaksi. Tällöin tietoverkossa toteutettua törkeää rahanpesukokonaisuutta ei voi verkossa menestyksellisesti tutkia.

Rikostorjunnan toimivaltakysymykset on avattu tarkemmin luvussa (4.5.2)

3.6.3.2 Identiteettirikollisuus, jonka tavoitteena on vahingoittaa kohdetta

Identiteettivarkaudet voivat ilmetä verkossa myös sellaisina koulu- ja työpaikkakiusaamisina, joissa ei synny taloudellisia tappioita eikä tavoitella taloudellista hyötyä.

Kiusantekotarkoituksessa toteutettu identiteettirikollisuus muistuttaa reaalielämän perinteistä identiteettirikollisuutta sikäli, että ilmiö tulee esiin yksittäistapauksina. Tekijän tavoitteena on vahingoittaa jotakin lähipiirinsä henkilöä kuten entistä puolisoa, koulukaveria, opettajaa, taikka jotakin julkisen vallan käyttäjää tai sellaiselta näyttävää tahoa. Tietoverkossa kunniaa tai yksityisyyttä loukkaava tieto voidaan kuitenkin saada leviämään paljon reaalimaailmaa suuremmalle joukolle. Loukkauksen välikappaleena käytetty tieto voi myös olla hyvin vaikeaa poistaa verkosta sen päästyä kerran leviämään riittävän laajalle. Tällöin teon vaikutukset voivat seurata rikoksen asianomistajaa kohtuuttoman kauan.

> Tästä esimerkkinä tapaus, jossa henkilö laittoi entisen puolisonsa yhteystiedot seksipuhelinsivustolle.

Tietoverkossa tapahtuva kiusanteko saattaa täyttää esimerkiksi kunnianloukkauksen (RL 24:9) tai yksityiselämää loukkaava tiedon levittäminen (RL 24:8) tunnusmerkistön.

3.6.3.3 Muu identiteettitiedon keruu ja väärinkäyttö tietoverkossa

”Muun identiteetin keruun ja väärinkäytön” muodostaa joukko sellaisia ilmiöitä, joissa ei voida nähdä ainakaan selkeää konkreettista hyötytarkoitusta ja joissa teon ensisijaise-

na tavoitteena ei ole aiheuttaa nimenomaista vahinkoa tietylle teon kohteena olevalle henkilölle. Tällöin tekijällä ei myöskään ole välttämättä lainkaan ymmärrystä siitä, että teosta saattaisi koitua uhrille mielipahaa tai muuta haittaa.

Joukkoon kuuluu hyvin erilaisia tekoja erilaisilla motiiveilla:

> 1. Verkon yhteisömedioiden myötä on noussut esille uusi ilmiö, jossa palveluun rekisteröidytään jonkin julkisuudenhenkilön nimellä ilman varsinaista vahingoittamistarkoitusta. Tiedollista itsemääräämisoikeutta on loukattu, kun joku luo yhteisöpalveluun profiilin käyttäen toisen henkilöllisyyttä tai ilmaisee mielipiteitä toisen henkilön nimellä. Kysymyksessä on kasvava ilmiö, kuten havaitaan uutisotsikoista ”kirjailija X suivaantui valeprofiilistaan Facebookista” tai ”ministeristä tehtiin valeprofiili nettiin”. Monet julkisuuden henkilöt ja tavalliset ihmisetkin ovat joutuneet tämän tapaisen toiminnan uhreiksi.
>
> Esille on tullut esimerkiksi tapauksia, joissa oppilas on tehnyt ajattelemattomuuttaan profiilin opettajansa nimissä ja opettajansa kuvalla ilman sen enempää tarkoitusta vahingoittaa kuin ymmärrystä seurauksista.
>
> Etenkin Facebook-yhteisöpalvelun valeprofiilien osalta ongelmana on sivuston ylläpitopaikka. Vaikka kunnianloukkauksen tunnusmerkistö täyttyisikin, yhdysvalloista IP-osoitteen saaminen on mahdollista vain hyvin rajoitetussa tapauksissa. Näin olleen kunnianloukkausjutut eivät etene, eikä tekijää saada kiinni vaikka itse rikosnimike täyttyisikin.
>
> Tiedollista itsemääräämisoikeutta on loukattu, kun joku luo yhteisöpalveluun profiilin käyttäen toisen henkilöllisyyttä tai ilmaisee mielipiteitä toisen henkilön nimellä – erityisesti mielipiteitä, joita henkilötietojen omistaja ei jaa. Tällainen tapaus saattaa myös loukata hyvinkin suoraan kohteen yksityisyyttä, jos joku kohteen todellinen tuttava ottaa verkkoprofiiliin yhteyttä ja tuo esiin kahdenvälisiä asioita kuvitellessaan keskustelevansa todellisen henkilön kanssa.
>
> 2. Toisena esimerkkinä ilmiöstä on taannoinen salasanankaappaustapaus, jossa 78 000 käyttäjätunnusta salasanoineen kaapattiin puutteellisesti suojatuilta palvelimilta. Tekijän motiivina ei ollut käyttää yksittäisiä tunnuksia ja salasanoja väärin ja siten loukata rekisteröityjen yksityisyyttä, vaan lähinnä osoittaa puutteita palvelinten turvallisuudessa. Tunnistetiedon julkistaminen verkossa oli kuitenkin omiaan vaarantamaan kaikkien tunnusten haltijoiden yksityisyyden sekä mahdollisesti myös yksityisen viestinnän, koska se mahdollisti helposti oikeudettoman kirjautumisen tunnukselle. Henkilörekisteririkoksen tunnusmerkistö ei tällaisessa teossa kuitenkaan oikeuskäytännön perusteella välttämättä täyty, sillä yksityisyyden loukkaaminen ei ole ollut rikoksentekijän tavoitteena.
>
> 3. Kolmas esimerkki muusta identiteettitiedon oikeudettomasta käytöstä on vuonna 2007 uutisoitu tapaus, jossa henkilö täytti toisen puolesta netissä olevan kirkosta-eroamisilmoituksen. Muutama erottaminen meni maistraateissakin läpi. Teko onnistuu kunhan erottaja tietää erotettavan nimen, kotiosoitteen ja henkilötunnuksen. Sähköpostillakin toisen erottaminen onnistuu, mikäli maistraatissa ei osata epäillä osoitetta vääräksi. Ilmaisen sähköpostiosoitteen voi hankkia kuka tahansa ja kenen nimellä tahansa. Kirkosta eroaminen onnistuu myös vapaa-ajattelijaliiton sähköistä kirkosta eroamislomaketta käyttämällä. Eroamisen voi toki mitätöidä ja maistraatista lähtee aina vahvistuskirje sähköisesti eronneelle, mutta teosta aiheutuu vaivaa kohteelle ja teko loukkaa henkilön oikeutta päättää tietojensa käytöstä.

Näyttäisi siltä, että tällaisissa tilanteessa mikään rikoslain tunnusmerkistö ei tarjoa teon uhrille suojaa, vaikka perustuslain 10 §:n mukaan jokaisen yksityiselämä, kunnia ja ko-

tirauha on turvattu. Erityisesti henkilötietojen suojasta säädetään tarkemmin lailla. Toisen henkilötietojen luvaton käyttö ilman taloudellisen hyödyn tarkoitusta tai suoranaista vahingoittamistarkoitustakin voi merkitä henkilön tiedollisen itsemääräämisoikeuden, eli siten myös yksityisyyden loukkaamista. Myös muun identiteettitiedon – kuten verkkopalvelun tunnistamistietojen – oikeudeton käyttäminen saattaa loukata samalla tavoin yksityisyyttä, vaikka jonkin yrityksen verkkopalvelun osoitetiedot eivät itsessään ole henkilötietoa. Verkkopalvelun identiteetin väärinkäyttämisellä voidaan kuitenkin tavoitella verkkopalvelun käyttäjien henkilötietoja.

3.7 Biometria

Biometriasta ei ole olemassa omaa erillistä yleislakia. Henkilötietolaki koskee yleislakina myös biometrisia tunnisteita, eikä niiden käyttöä ole suljettu pois myöskään lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista soveltamisalan ulkopuolelle.

Valtioneuvoston periaatepäätöksessä sähköisestä tunnistamisesta ovat mukana myös biometriset tunnisteet ja siihen liittyvä lainsäädännön tarve.

> 7) Biometristen tunnisteiden käyttäminen sähköisessä tunnistamisessa
> Biometrinen tieto liittyy poikkeuksellisen kiinteästi yksilöön itseensä ja on siten luonteeltaan hyvin toisenlaista kuin muu henkilötieto. Biometrisen tunnisteen menettämiseen liittyy peruuttamattomuus.
>
> Voimassa oleva lainsäädäntö ei ota riittävästi huomioon biometriseen tunnistamiseen liittyviä erityispiirteitä. Lainsäädäntö ei anna palvelujen kehittäjille riittävää ohjausta palvelujen toteuttamiseksi tunnistettavien yksityisyyden suojan turvaavalla tavalla. Palvelujen kehittäjien on käytännössä vaikeaa arvioida voimassa olevasta sääntelystä, miten ja mihin biometrista tunnistamista voi käyttää ja miten palvelut tulisi toteuttaa tunnistettavien yksityisyyden suoja huomioon ottavalla tavalla. Oikeustilan epäselvyys on selvä riski kansalaisten yksityisyyden suojalle. Jos biometrista tunnistamista koskevia pelisääntöjä ei lainsäädännöllä selkeytetä, uhkana on, että Suomenkin markkinoille tuodaan yhä enenevässä määrin biometrista tunnistamista hyödyntäviä palveluja, joissa tunnistettavien yksityisyyden suojaan ja tietoturvaan liittyviä vaatimuksia ei ole huomioitu riittävässä määrin. Alan pelisääntöjä selkeyttämällä turvattaisiin kansalaisten yksityisyyden suoja biometrisen tunnistamisen käytössä.
>
> Tavoitteet:
> Biometristen tunnisteiden käyttöä säännellään jatkossa yleisesti siten, että voidaan turvata kansalaisten yksityisyyden suojan ja tietoturvan vaatimukset niiden käyttämisessä. Biometristen tunnisteiden käyttäminen ei liity pelkästään vahvan sähköisen tunnistuspalveluiden tarjontaan, vaan niitä voidaan käyttää ja parhaillaan jo käytetään myös toimijoiden omissa sisäisissä järjestelmissä esimerkiksi kuntosaleilla. Tämän johdosta sääntelyn oikea paikka ei ole valmisteilla oleva laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, vaan sääntelyn olisi oltava horisontaalista. Tarvittavat yleiset säännökset biometristen tunnisteiden käsittelystä olisi tältä kannalta aiheellista sijoittaa henkilötietolakiin.

Keinot:
Oikeusministeriö asettaa vuoden 2009 aikana työryhmän selvittämään asiaa. Työryhmässä ovat edustettuina ainakin liikenne- ja viestintäministeriö, sisäasiainministeriö ja valtiovarainministeriö.

Tällä hetkellä myönnettävistä asiakirjoista biometrisiä tunnisteita hyödynnetään ainoastaan passeissa. Erityislaissa (passilaki) on säädetty kasvokuvasta sekä sormenjälkien ottamisesta. Kansallisen passilain biometristen tunnisteiden ottamisen takana on EU:n passiasetus: Neuvoston asetus (EY) N:o 2252/2004 jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista. Jatkossa biometriset tunnisteet tulevat myös oleskelulupiin. Myös henkilökortteihin on suunniteltu lisättäväksi biometriset tunnisteet.

Myös viisumeja varten ryhdytään ottamaan sormenjälkiä. Viisumi on maahantulolupa, jota haetaan ensisijaisesti hakijan kotimaassa olevasta Suomen edustustosta. Ulkomaalaisen Suomeen tuloon ja maassa oleskeluun sovelletaan mitä ulkomaalaislaissa (301/2004) ja Schengenin säännöstössä määrätään. Viisumeiden osalta raportissa tuodaan esille vain uusi viisumitietojärjestelmä ja siihen liittyvät biometriset tunnisteet. Tästä osiosta kerrotaan enemmän osiossa 4.6.1.1.

Biometrian hyödyntämisen edellytyksenä on luotettava linkki ihmisen fyysisten ominaisuuksien ja identiteetin (nimi ja muut henkilötiedot) välille. Linkki muodostuu, kun myöntövaiheessa varmistetaan, että identiteettiin varmasti liitetään oikean ihmisen biometriset tunnisteet.

Biometriaa voidaan hyödyntää jo luotettavan linkin muodostamisvaiheessa. Uuden asiakirjan myöntövaiheessa voidaan hakijalta kerättäviä tietoja verrata joko hakijasta jo valmiiksi rekisterissä oleviin tunnisteisiin tai hänellä ennestään olevan asiakirjan biometrisiin tunnisteisiin. Vertaamalla kerättäviä biometrisia tunnisteita muihin rekisterissä oleviin tunnisteisiin pyritään estämään kahden tai useamman henkilöllisyyden käyttö.

Suomessa passisiruissa olevia biometrisiä tunnisteita käytetään osassa Schengenin ulkorajatarkastuksissa ja muissa passintarkastustilanteissa vertaamalla passissa olevia biometrisia tunnisteita passinhaltijan fyysisiin ominaisuuksiin. Rajatarkastuksissa tapahtuvan tunnistuksen turvallisuus nojaa täydellisesti myöntövaiheessa luotuun luotettavaan linkkiin.

Rajavartiolaitos käyttää biometrisiä tunnisteita rajatarkastuksissaan. Rajavartiolaitoksen keskeisenä strategisena tavoitteena on ottaa hallitusti käyttöön pääosin automatisoitu ja tuottavuutta parantava rajatarkastus. Rajavartiolaitoksella on henkilötietojen käsittelystä rajavartiolaitoksesta annetun lain (579/2005) nojalla oikeus ottaa vastaan henkilön fyysisiin ominaisuuksiin perustuva matkustusasiakirjaan liitetty sähköinen tunniste henkilön tunnistamista ja asiakirjan aitouden varmistamista varten.

Rajavartiolaitos on hyväksynyt operatiiviseen käyttöön EU/ETA/CH kansalaisille suunnatun automaattisen rajatarkastusjärjestelmän. Järjestelmän käyttöönottoa edelsi mainituille kansalaisille suunnattu pilottikokeilu Helsinki-Vantaan lentoasemalla vuonna 2008. Järjestelmä suorittaa automaattisesti Schengenin rajasäännöstön mukaisen vähimmäistarkastuksen. Vuonna 2009 käynnistettiin hanke, jonka toiminnallisena tavoitteena on selvittää automaattisen rajatarkastuksen soveltuvuutta laajemmin Schengenin ulkorajan henkilöliikenteen rajatarkastuksiin. Käytännön tavoitteena on automaattinen rajatarkastusjärjestelmä, joka soveltuu kaikkien biometrisesti tunnistettavien matkustajien Schengenin rajasäännöstön mukaisiin rajatarkastuksiin. Rajavartiolaitos varautuu suorittamaan rajatarkastusten yhteydessä viisumivelvollisten sormenjälkiverifikaatiot EU:n VIS-asetuksen mukaisesti. Hankkeessa huomioidaan myös muut EU:n rajaturvallisuushankkeet.

4 Kehitysnäkymät ja riskit

4.1 Henkilöllisyyden luominen

Syntymän kautta saatavan henkilöllisyyden osalta työryhmä ei havainnut ongelmia. Työryhmässä vallitsi yhtenäinen näkemys siitä, että jokaisella voi olla Suomessa vain yksi henkilöllisyys, jota hän demonstroi niin henkilökohtaisessa kanssakäymisessä kuin sähköisestikin. Lisäksi henkilöllä voi sähköisessä maailmassa olla useita identiteettejä, jotka hän itse luo, ja joilla joko on tai ei ole yhtymäkohtia hänen todelliseen henkilöllisyyteensä.

Ulkomaalaisen henkilön henkilöllisyyden rekisteröinti Suomessa tulee lähtökohtaisesti perustua ulkomaalaisen esittämiin luotettaviin asiakirjoihin. Ulkomaalaisen henkilön henkilöllisyys ja henkilöllisyyteen liittyvät henkilötiedot tulisivat näin ollen olla samat asuinvaltiosta riippumatta. Väestörekisteriin merkitsemisen ja henkilötunnuksen antamisen ei lähtökohtaisesti pitäisi synnyttää ulkomaalaiselle henkilölle uutta henkilöllisyyttä, mutta tämä mahdollisuus on olemassa, kun oleskeluluvan ilman luotettavaa henkilöllisyyden osoittavaa asiakirjaa saanut ulkomaalainen rekisteröidään väestötietojärjestelmään. Luotettavana pidettävän näytön puuttuessa on mahdollista, että ulkomaalaisella henkilöllä voi olla omassa maassaan toinen henkilöllisyys tai jotkut hänen henkilöllisyyteensä liittyvät tiedot poikkeavat siitä, mitä hän on ilmoittanut Suomen viranomaiselle. Virallisten asiakirjojen puuttuessa viranomaiset eivät voi varmistua tietojen oikeellisuudesta eivätkä näin ollen välttämättä saa tietoonsa ulkomaalaisen todellista henkilöllisyyttä tai oikeita henkilötietoja.

4.1.1 Ulkomaalaisen varmistamaton henkilöllisyys

4.1.1.1 Terminologia

Ulkomaalaisten osalta erityistilanteita syntyy, koska kaikkien henkilöiden osalta (esimerkiksi turvapaikanhakijat ja pakolaiset) henkilöllisyyttä ei pystytä luotettavasti varmistamaan. Varmistamattomasta henkilöllisyydestä käytettävät termit ovat poikkeavia eri lainsäädännöissä ja se on omiaan aiheuttamaan ongelmia. Näitä eri laeissa käytettyjä eri termejä ei ole sisällöllisesti määritelty.

Ulkomaalaislain 136 §:n 5 momentin mukaan: ”Jos ulkomaalaisen henkilöllisyyttä ei ole pystytty varmistamaan, siitä tehdään merkintä muukalaispassiin tai pakolaisen matkustusasiakirjaan”. Kyseessä on erityissäännös, joka mahdollistaa matkustusasiakirjan myöntämisen ulkomaalaiselle, jolle on voitu myöntää oleskelulupa Suomeen siitä huolimatta, että hänen henkilöllisyyttään ei ole voitu varmistaa. Ulkomaalaislain mukainen matkustusasiakirja myönnetään ulkomaalaiselle muussa kuin henkilöllisyyttä osoittavan asiakirjan ominaisuudessa.

Henkilökorttilain 1 §:n mukaan: Poliisi antaa hakemuksesta todistuksen henkilöllisyydestä (henkilökortti) Suomen kansalaiselle ja kotikuntalain (201/1994) mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle, joka on merkitty väestötietojärjestelmään ja jonka henkilöllisyys on voitu luotettavasti todeta. Henkilökorttia ei luonteensa perusteella voida myöntää sillä varauksella, että henkilöllisyyttä ei ole pystytty varmistamaan.

Kansalaisuuslain (359/2003) 6 §:n 1 momentin mukaan: Suomen kansalaisuuden saaminen edellyttää, että henkilöllisyys on luotettavasti selvitetty. Selvitystä henkilöllisyydestä voidaan 2 momentin mukaan esittää asiakirjanäytöllä tai antamalla muutoin luotettavina pidettäviä tietoja asianomaisen henkilön nimestä, syntymäajasta, perhesuhteista ja muista asian ratkaisemisen kannalta tarpeellisista henkilötiedoista. Henkilöllisyyttä selvitettäessä voidaan ottaa huomioon ne tiedot, jotka henkilö on aikaisemmin antanut viranomaiselle omasta ja lapsensa henkilöllisyydestä". Tämä liittyy siis ainoastaan kansalaisuuden myöntämiseen. Se, että kansalaisuus voidaan myöntää, ei välttämättä kerro vielä mitään siitä, onko hakijan henkilöllisyys voitu luotettavasti todeta/varmistaa. Kansalaisuuslain mukaan 6 §:n 3 momentin mukaan: Jos ulkomaalainen on vähintään viimeksi kuluneet 10 vuotta esiintynyt väestötietojärjestelmästä ilmenevällä henkilöllisyydellä, hänen henkilöllisyyttään pidetään 1 momentin mukaisesti selvitettynä, vaikka hän olisi aiemmin esiintynyt useammalla kuin yhdellä henkilöllisyydellä. Kansalaisuuslaissa on "selvitetty henkilöllisyys" -määritelmän avulla mahdollistettu Suomen kansalaisuuden myöntäminen myös tilanteissa, joissa ulkomaalaisen henkilöllisyyttä ei ole pystytty varmistamaan.

Kokonaiskuvan muodostaminen on tärkeää, koska epäselvä/todentamaton henkilöllisyys vievät paljon resursseja alussa, mutta myöhemmin kansalaistamisvaiheessa epäselvä henkilöllisyys tai /ja varmistamaton henkilöllisyys "hyväksytään" eli legalisoidaan. Kansalaistamisen yhteydessä tapahtuva legalisointi ei kuitenkaan ole lopullinen. Kansalaisuuslain 33 §:n 1 momentin mukaan kansalaisuuden saanut henkilö voi menettää Suomen kansalaisuutensa väärien tietojen antamisen perusteella. Henkilöllisyyden kokonaishallinta on vaikeaa. Termien moninaisuus selittyy osittain myös EU-lainsäädännöllä, sillä kansallisessa implementoinnissa on tapana käyttää täysin samoja termejä kuin vastaavassa direktiivissä.

Turvapaikkatutkinnassa poliisi ja rajavartiolaitos selvittävät turvapaikanhakijan henkilöllisyyttä, matkareittiä ja maahantuloa. Selvityksen lopputuloksena ei kuitenkaan henkilöllisyyden osalta vaihtoehtoina ole selvitetty henkilöllisyys tai ei selvitetty henkilöllisyys. Lopputulosvaihtoehdot suoritetun selvityksen perusteella ovat: Henkilöllisyys on varmistettu tai henkilöllisyyttä ei ole pystytty varmistamaan. Kansalaisuuslain termi "luotettavasti selvitetty henkilöllisyys" tulisi erottaa ulkomaalaislain systematiikasta. Kansalaisuuslain "epäselvä henkilöllisyys -harkinta" aktualisoituu tilanteissa, joissa ulkomaalainen on esiintynyt useammalla kuin yhdellä henkilöllisyydellä ja liittyy usein asumisajan laskemiseen.

Esimerkkejä: 1) Ulkomaalainen, jonka henkilöllisyyttä ei ole voitu varmistaa maahan tullessa, esittää kotimaansa luotettavan passin 5 vuoden jälkeen maahan tulostaan. Passista ilmenee, että ulkomaalaisen henkilötiedot poikkeavat alun perin esitetystä. Nyt hakijan henkilöllisyydestä on pystytty varmistumaan, mutta kansalaisuuslain asumisaika aletaan laskea vasta siitä lähtien, kun oikea henkilöllisyys on tullut viranomaisten tietoon. 2) Maahan tulleen ulkomaalaisen henkilöllisyyttä ei ole pystytty varmistamaan, mutta hän on esiintynyt koko ajan samoilla henkilötiedoilla. Ulkomaalainen voidaan kuitenkin kansalaistaa, vaikka hänen henkilöllisyyttään ei ole voitu varmistaa, koska esteet kansalaistamiselle liittyvät eri henkilöllisyydellä esiintymiseen, ei siihen, että henkilöllisyyttä ei ole voitu varmistaa. Kansalaisuuslain 10 vuoden sääntökin liittyy tähän samaan asiaan: Oleellista kansalaisuuslaissa on tietojen pysyminen samana, ei niiden todellinen varmistaminen.

Määritelmien kontekstierot ovat olennaisia ja esimerkiksi kansalaisuuslain analogian käyttäminen esim. matkustusasiakirjojen merkintöjä koskevassa soveltamisessa aiheuttaa virheitä ja väärinkäsityksiä. Pääsääntöisesti kansalaisuuslain analogia tulisi pitää kokonaan erossa ulkomaalaislain ja tietysti myös henkilökorttilain analogiasta.

Henkilötietojen pysyvyydellä on merkitystä tarkasteltaessa asiaa etenkin kansalaisuuslain näkökulmasta. Kansalaistamisvaiheessa viranomaisella on käytettävissä kaikki henkilöstä löytyvä asiakirjamateriaali. Henkilöllisyyden selvyyden arvioimisessa otetaan huomioon myös maahantulovaiheessa kerrotut tiedot. Tässä mielessä tietojen "jäädyttämisellä " jo hyvin varhaisessa vaiheessa on merkitystä myöhemmin arvioitaessa sellaisen henkilön henkilöllisyyttä, joka on tullut maahan ilman henkilöllisyyttä osoittavia asiakirjoja.

4.1.2 Ulkomaalaisen varmistamaton henkilöllisyys ja asiointi

Ratkaisuna (osiossa 3.2.2.2) turvapaikanhakijoiden asiointiongelmaan turvapaikkaprosessin aikana ulkomaalaistyöryhmä on keskustellut ”turvapaikanhakijoiden asiointikortista”, joka annettaisiin turvapaikanhakijoille, joiden henkilöllisyyttä ei ole voitu varmistaa. Turvapaikanhakijan asiointikorttia ei kuitenkaan alustavan arvion perusteella myönnettäisi turvapaikanhakijoille, jotka ovat unionin kansalaisia tai joiden hakemuksen käsittelystä on vastuussa toinen Euroopan unionin jäsenvaltio. Asiointikortin myöntäminen mainittuihin ryhmiin kuuluville turvapaikanhakijoille ei olisi tarkoituksenmukaista lyhyen Suomessa oleskelun ja myös kustannussyiden vuoksi. Alaikäisten turvapaikanhakijoiden osalta tulee lisäksi harkita, kenelle heistä asiointikortin myöntäminen on tarkoituksenmukaista.

Turvapaikanhakijan asiointikortista säädettäisiin erikseen laissa (esim ulkomaalaislaki). Kortti sisältäisi biometriset tunnisteet; sormenjäljet ja kasvokuvan. Turvapaikanhakijan henkilöllisyys jäädytettäisiin biometristen tunnisteiden ja ilmoitettujen henkilötietojen

mukaisena kokonaisuutena yhteen henkilöllisyyteen ja tätä henkilöllisyyttä käytettäisiin viranomaisissa ja esimerkiksi pankeissa asioidessa.

Kortti olisi polykarbonaattikortti ja normaalin pankkikortin kokoinen. Kortti ei olisi passiin tai henkilökorttiin verrattava henkilöllisyyttä osoittava asiakirja, vaan pelkästään asiointikortti lähinnä nykyisen vastaanottokeskusten pahvikortin tilalle. Kortti mahdollistaisi asioinnin eikä sillä olisi muita toimintoja. Se ei siis mahdollistaisi esimerkiksi työntekoa, josta säädetään erikseen ulkomaalaislaissa. Korttiin tulisi merkintä varmistamattomasta henkilöllisyydestä. Kortti myönnettäisiin määräaikaisena ja sen todellinen käyttöaika rajattaisiin kortin myöntöpäivän ja maasta poistumisen väliselle ajalle tai kortin myöntöpäivän ja muukalaispassin, pakolaisen matkustusasiakirjan tai kansallisen passin myöntämisen väliselle ajalle. Kun henkilö saa muukalaispassin, pakolaisen matkustusasiakirjan tai kotivaltionsa kansallisen passin tai hän saa kielteisen oleskelulupapäätöksen ja joutuu poistumaan maasta, kortti tulisi palauttaa ja peruuttaa. Tunnistetietona kortissa käytettäisiin ulkomaalaisrekisterin asiakasnumeroa, ei henkilötunnusta. Korttiin tulisi myös merkintä siitä, että se on voimassa vain Suomessa.

Toimivaltainen viranomainen myöntämään kortti olisi poliisi. Tärkeää olisi, että kortin voimassa olo lakkaisi henkilön maasta poistumisen yhteydessä ja tästä tehtäisiin merkintä UMA-järjestelmään. Asiointikortti tulisi myös olla mitätöitävissä, jos selviää, että kortinhaltijan todellinen henkilöllisyys on täysin toinen, jonka perusteella kortti on myönnetty. Mitätöinti tulisi kyseeseen esimerkiksi tapauksissa, joissa turvapaikanhakija on esiintynyt toisen todellisen henkilön tiedoilla tai hän on esiintynyt henkilönä, jota todellisuudessa ei ole olemassa. Kortin voimassa olon lakkauttamisella ja mitätöimisellä varmistettaisiin se, että korttia ei voisi käyttää väärin myöhemmin ja merkinnät lakkauttamisesta tai mitätöimisestä välitettäisiin järjestelmien välisessä tietojenvaihdossa. Kortin voimassa olon lakkaaminen tai mitätöiminen ei välttämättä vaikuttaisi mahdollisiin väärinkäytöksiin ulkomailla ja etenkin edustustot olisi informoitava kortista hyvin ennen mahdollista käyttöönottoa. Kortin haltuun saaminen olisi tärkeää myös kotimaisten toimijoiden kannalta. Esimerkiksi yksityisillä toimijoilla ei ole pääsyä poliisin tietojärjestelmiin, joten he eivät voi tarkistaa sitä, onko kortti tietojärjestelmässä mitätöity tai onko henkilölle myönnetty jokin muu asiakirja. Kortin haltuun saaminen onkin haaste.

Henkilöllisyyden jäädyttämishetki on sovittava ja selvitettävä erikseen, mutta sen tulisi olla mahdollisimman pian henkilön maahan saapumisen jälkeen. Tällä on resurssivaikutuksia muun muassa turvapaikkakuulusteluihin. Koska kortti palautettaisiin pois, se voisi olla tällöin myös ulkomaalaislain 96 §:n mukainen osoitus asian vireilläolosta, mutta pääasiallisesti asiointikortti. Sisäasiainministeriön poliisiosasto on henkilökorttikilpailutuksen yhteydessä jo kilpailuttanut myös turvapaikanhakijan asiointikortin. Asiointikortin käytännön toimintapahoihin sekä lainsäädäntöön liittyvät kysymykset on pohdittava erikseen. Myös resurssivaikutukset täsmentyvät ajan myötä.

Henkilöllisyyden jäädyttäminen vaatii biometristen tunnisteiden käyttöä, jotka yhdistetään henkilöstä saatuihin tietoihin (henkilöllisyysdokumentit tai oma ilmoitus). Tällaisia

biometrisia tunnisteita voivat olla kasvokuva, sormenjälki, sormen sisällä kulkevat verisuonet, silmän iiris jne. Henkilöllisyyteen tulisi yhdistää aina useampi biometrinen tunniste, joita ei koskaan yksinään käytetä henkilöllisyyden selvittämiseksi. On kuitenkin samalla huomioitava, ettei Suomesta saa tulla maata, jossa myönnetään ns. uusi henkilöllisyys liian helposti.

Ongelman ydin on, ettei suurin osa turvapaikanhakijoista esitä henkilöllisyyttä osoittavia asiakirjoja, joten kaikkien osalta henkilöllisyyden varmistaminen ei onnistu koskaan.

4.2 Tunnistaminen fyysisessä ja sähköisessä toimintaympäristössä

Luotettavan henkilöntunnistuksen tarve voidaan jakaa kahteen ryhmään, joista ensimmäinen liittyy 1) läsnä olevan henkilön tunnistamiseen ja toinen 2) verkkoasioinnin yhteydessä tapahtuvaan tunnistamiseen. Jako on tarpeellinen, koska jälkimmäisessä ei ole käytettävissä samoja menetelmiä kuin ensin mainitussa. Läsnä oleva henkilö voidaan esimerkiksi tunnistaa biometrisesti, koska biometrinen näyte voidaan tällöin ottaa valvotusti, mutta verkkoasioinnissa tämä ei ole mahdollista. Muutoin suurin osa tunnistamiseen liittyvistä riskeistä koskee kuitenkin yhteisesti kumpaakin toimintaympäristöä, kun kyse on itse tunnistamistapahtumasta. Vahvan sähköisen tunnistamisen varmenteetkin perustuvat viranomaisen myöntämiin fyysisiin asiakirjoihin.

Henkilön tunnistaminen sekä kasvotusten että sähköisessä toimintaympäristössä on olennaista turvallisen asioinnin ja kansalaisten oikeusturvan kannalta. Henkilöllisyyden ja tunnistamisen kannalta kansalaisen oikeusturvan tulee olla samalla tasolla, huolimatta siitä onko kyse fyysisestä vai sähköisestä toimintaympäristöstä. Oikeustoimet ovat yhtä sitovia riippumatta käytettävästä välineestä.

Ensimmäistä kertaa tehtävä tunnistaminen on kriittinen vaihe niin tunnistamisasiakirjoja kuin sähköisiä varmenteitakin myönnettäessä. Sähköinen toimintaympäristö on muovannut tunnistamiskenttää nopeasti. Kansalaiset käyttävät paljon sähköisiä palveluita, joiden tunnistamisaste ja -tavat ovat hyvin erilaisia. Kansalaisen on vaikea tietää, mikä palvelu on luotettavaa ja mikä ei. Tietovarkaudet ovat arkipäivää, mutta kiinnijäämisen riski on olematon. Fyysiset asiakirjat ovat tuttuja ja niiden väärentäminen on helposti hahmotettavissa. Tietoverkoissa tapahtuvat tietomurrot tai henkilötietojen kalastelu eivät ole samalla tavalla havaittavissa.

1) Poliisin myöntämien henkilöllisyyttä osoittavien asiakirjojen (passi ja henkilökortti) osalta henkilön tunnistaminen on prosessin tärkein vaihe. Tunnistaminen onkin syytä tehdä fyysisessä toimintaympäristössä luotettavista tunnistamisasiakirjoista, muuten myönnettyyn asiakirjaan ei voi luottaa.

Käytännössä fyysisten asiakirjojen kohdalla suurin ongelma on näennäistunnistaminen, jossa esimerkiksi vain katsotaan tunnistamisasiakirjasta henkilötunnuksen loppuosa, mutta ei verrata nimiä tai katsota onko kuvassa oikea henkilö. Tunnistamisasiakirjoja on myös paljon, etenkin ulkomaalaisia passeja, joten tunnistaminen vaatii erityisosaamista ja koulutettua henkilöstä.

Pidemmän tähtäimen tavoitteena tulisi olla sellaisten tunnistusjärjestelmien luonti, joissa tekniset tunnistusjärjestelmät toimivat ihmisen apuna tunnistamistilanteessa, mutta tunnistamisen ei tule koskaan perustua pelkästään teknisen laitteen arvioon, kun on kyse henkilöllisyyttä osoittavan asiakirjan myöntämisestä tai ensitunnistamisesta. Ulkomaalaiset väärennetyt tunnistusasiakirjat aiheuttavat enemmän ongelmatilanteita kuin kotimaiset, sillä erilaisia passeja on suuri määrä ja aitojen kappaleiden turvataso saattaa alun perin olla heikko. Kotimaisia passeja ja henkilökortteja väärennetään harvoin, sillä niiden turvataso on hyvin korkea, minkä lisäksi aidoista asiakirjoista on hyvin saatavilla mallikappaleita vertailuja varten. Ulkomaalaisten tunnistusasiakirjojen aitouden toteamiseen liittyviä ongelmia voidaan merkittävästi vähentää hankkimalla poliisille ja muille viranomaisille asiakirjanlukulaitteita, jotka on varustettu havaitsemaan väärennökset. Poliisihallitus on jo hankkimassa asiakirjalukulaitteitteita paikallispoliisille. Tämä hankinta on myös mainittu lupahallinnon toimena myös laittoman maahantulon vastaisessa toimintaohjelmassa.

2) Myös sähköisessä toimintaympäristössä (vahva sähköinen tunnistaminen) ensitunnistaminen on keskeistä, kun viranomainen myöntää tai yksityinen palveluntarjoaja antaa asiakkaalle sähköisiä varmenteita ja myös tällöin tunnistamisasiakirjat ovat olennaisessa roolissa. Luotettava verkkoasiointi on mahdollista vain, jos verkkotunnistautumisessa käytettävä tunniste on riittävän vahva ja se on alun perin luovutettu oikealle henkilölle. Näin ollen verkkoasioinnin luotettavuus riippuu ratkaisevasti keinoista, joilla sähköisen tunnisteen ensihakija on tunnistettu hänen ollessaan fyysisesti läsnä hakemuksenjättöpaikassa. Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 66 § sääntelee kansalaisvarmenteen hakemista ja myöntämistä ja vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 17 § säätelee ensitunnistamista. Tulevaisuudessa vahvan sähköisen tunnistamisen merkitys kasvaa entisestään.

4.2.1 Riskianalyysi tunnistamisprosessiin liittyvistä riskeistä

Hanke on teettänyt asettamiskirjeen mukaisesti riskianalyysin tunnistamisprosessiin liittyvistä riskeistä. Toimeksianto sisälsi myöntöprosessin tarkastelun (tunnistaminen ja siinä käytettävät tunnistamisasiakirjat) passin, henkilökortin ja ajokortin sekä kansalaisvarmenteen osalta. Toimeksianto sisälsi myös passin myöntämisen edustustoissa sekä kadonneiden ja anastettujen asiakirjojen puutteet. Muiden varmenteiden osalta riskianalyysiä ei ole tehty. Liikenne- ja viestintäministeriö on katsonut, ettei riskinanalyysi ole

enää tässä vaiheessa muiden varmenteiden osalta tarpeellinen, koska laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista on jo voimassa.

Riskianalyysin teki yksityinen konsulttitoimisto ja työtapoina olivat työpajat, haastattelut sekä tehdyt dokumentaatiot. Haastateltavat olivat sisäasiainministeriöstä, ulkoasiainministeriöstä, Maahanmuuttovirastosta sekä poliisilaitoksilta ja kaikilla oli käytännön asiakaspalvelutyöstä kokemusta.

Riskianalyysissä tulivat esille seuraavat keskeisimmät riskit:

1. Ajokortin hyväksyminen tunnistamisasiakirjaksi
2. Inhimillinen erehdys
3. Virkailijoiden kiire
4. Tunnistamisen tason vaihteleminen toimipisteittäin
5. Henkilön tunnistaminen tehdään puutteellisin perustein
6. Tunnistamiseen kelpaavien asiakirjojen puuttuminen ulkomaalaiselta
7. Tunnistamiseen käytettävän asiakirjan kuvaa ja muita yksilöintitietoja ei verrata huolellisesti hakijaan
8. Tarkoituksellinen virkailijan harhauttaminen
9. Väärennetyn asiakirjan esittäminen
10. Ulkomaalaiset henkilöt muuttavat tietojaan maistraatissa tiheään

Kohdat 1 ja 2 arvioitiin sietämättömiksi riskeiksi ja kohdat 3-10 merkittäviksi riskeiksi. Kohdan 10 osalta todetaan, että uusi laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista on tuonut tältä osin parannusta tilanteeseen.

Poliisihallitus tulee ottamaan riskianalyysin tulokset huomioon alaisen hallintonsa toimintaprosesseissa ja koulutuksessa.

4.3 Tunnistamisasiakirjat

4.3.1 Kela-kortti

Kela on jo lopettanut kuvallisten Kela-korttien myöntämisen, mutta niitä on voimassaolevina vielä kansalaisilla erittäin paljon. Työryhmä katsoo, ettei Kela-korttia tulisi lainkaan käyttää henkilöllisyyden osoittamiseen sen huonon turvatekijätason ja myöntöprosessin heikkouden takia. Kela-korttia käytetään edelleenkin varsin paljon tunnistamisasiakirjana, etenkin ikäihmisten osalta, joilla ei ole ajokorttia tai voimassa olevaa matkustusasiakirjaa. Työryhmä katsoo kuitenkin, että myös tämän ikäryhmän asiointi on mahdollistettava jollakin muulla turvallisella tavalla.

4.3.2 Ajokortti

Sisäasiainministeriö on asetustasoisesti katsonut, ettei ajokorttia ole tarkoitettu tunnistamisasiakirjaksi, eikä sen myöntöprosessi ole niin turvallinen, että sen käyttö tunnistamisasiakirjana olisi jatkossa perusteltua. Asiaintilan muuttaminen edellyttäisi sitä, että toisaalta palveluntarjoajat hyväksyisivät henkilöllisyyden osoittamiseen ainoastaan siihen tarkoitetut asiakirjat, eli passin tai henkilökortin. Toisaalta edellytyksenä olisi, että Suomessa asuvat henkilöt kantaisivat yleisesti mukanaan jompaakumpaa näistä.

Tähän saakka puhtaasti kotimaisen ajokortin väärinkäyttöön tunnistamisasiakirjana liittyvät tapaukset ovat olleet kohtuullisen vähäisiä, mutta on syytä arvioida, että jatkossa väärinkäytösten määrä on kasvussa. Suurin väärinkäytösriski sisältyy ulkomaisista korteista vaihdettuihin ajokortteihin. KRP rikostekninen laboratorio tutkii väärennettyjä ja väärennetyksi epäiltyjä asiakirjoja. KRP:n rikosteknisessä laboratoriossa vuonna 2008 tutkituista ulkomaalaisista ajokorteista 49 % on todettu väärennetyiksi. Vuonna 2009 KRP totesi vääriä tai väärennettyjä ulkomaalaisia ajokortteja yhteensä 266 kappaletta. Kotimaisia ajokortteja KRP ei pääosin tutki, koska paikallispoliisi pystyy selvittämään rekistereistä onko kortti aito vai ei.

Poliisiasiain tietojärjestelmä ei ole rakenteeltaan paras tilastojärjestelmä ja ajokorteilla tehdyt rikokset ovat pääosin piilorikollisuutta, joten luvut kertonevat vain osan totuudesta. Kokonaiskuvaa tilanteesta antavaa tilastotietoa poliisilla ei siis ole tällä hetkellä saatavissa.

Ajokorttia koskeva lainsäädäntö tulee kokemaan merkittäviä muutoksia. Uuden ajokorttidirektiivin on tultava kansallisesti voimaan 19.1.2013. Tällöin muun muassa kaikki ajokortit muuttuvat määräaikaisiksi: kuorma-auton ja sitä raskaampien ajoneuvojen ja ajoneuvoyhdistelmien ajo-oikeus on voimassa 5 vuotta, ja pienempien ajoneuvoluokkien ajokortit ovat voimassa 15 vuotta nykyisen 70 vuoden sijaan. Hallituksen esitys ajokorttilaiksi ja eräiksi siihen liittyviksi laeiksi (HE 212/2010) on eduskuntakäsittelyssä. Lainsäädäntöuudistus tuo muutoksia sekä ajokortin myöntöprosessiin että ajokortin luovuttamiseen. Esitys ajokorttilaiksi tuo mukanaan uudistuksen, jossa ajokortit postitetaan suoraan valmistajalta asiakkaalle vuoden 2013 alusta lähtien. Samassa yhteydessä Liikenteen turvallisuusvirasto ja Poliisihallitus toteuttavat ajokorttiasioiden sähköisen asioinnin.

Poliisihallitus ja Liikenteen turvallisuusvirasto uudistavat ajokortin myöntämismenettelyitä liikenteen tietojärjestelmän kokonaisuudistuksen yhteydessä. Myöntöprosessia tullaan entisestään keventämään siirtymällä sähköiseen myöntöprosessiin. Menettely tulee perustumaan kansalaisen asiointitiliin, joka on valtiovarainministeriön hanke. Vuodesta 2013 lähtien poliisi tuleekin myöntämään vuodessa pelkästään 700 000 ajokorttia ja kortit postitetaan suoraan hakijalle. Muutoksilla on olennaista vaikutusta ajokortin hyväksyttävyyteen tunnistamistilanteissa.

Ajokortin käyttöön liittyvät ongelmat:

1. Myöntöprosessi: Myöntöprosessi ei ole samantasoinen kuin passilla ja henkilökortilla, koska siihen ei sisälly viranomaisen tekemää tunnistusta. Ajokortin hakijan henkilöllisyyden tarkistaa ajokorttihakemuksen yhteydessä autokoulussa yksityinen toimija.

2. Turvataso: Ajokortti on turvatekijöiltään vähäinen ja siten helposti väärennettävä. Houkutus ajokortin väärentämiseen kasvaa, jos/kun sitä voi käyttää tunnistamisasiakirjana, jolla taas voi tehdä sitovia oikeustoimia.

3. Voimassaoloaika: Ajokortin voimassaoloaika (70 vuotta) ei vastaa passin tai henkilökortin voimassaoloaikaa (5 vuotta). Uusi ajokorttidirektiivi lyhentää ajokortinvoimassaoloaikaa 5-15 vuodeksi. Ammattiautoilijoiden osalta voimassaoloaika tulee olemaan 5 vuotta ja muilla 15 vuotta.

4. Kansalaisuus: Ajokortista ei käy ilmi henkilön kansalaisuus, vaan myöntävän valtion kansallistunnus.

5. Ajokortin asema tunnistamisasiakirjana: Tällä hetkellä yleisin tunnistamiseen käytettävä asiakirja on ajokortti, vaikka sitä ei ole sellaiseksi tarkoitettu. Lähes kaikki palveluntarjoajat hyväksyvät ajokortin. Esimerkiksi kaupat ovat laajasti hyväksyneet ajokortin maksutapahtuman varmentamisessa. Tällöin kuitenkin väärällä/väärennetyllä ajokortilla tehdystä ostosta vastaa kauppa tai kortin myöntänyt yhtiö, ei asiakas itse. Kyse on siis yksityisestä riskienhallinnasta. Monissa muissa tilanteissa kuluttaja voi kuitenkin joutua itse vastuuseen väärinkäytöksistä. Keskeistä on, ettei huonolla/väärällä asiakirjalla tehdystä tunnistamisesta aiheutuva riski jää kansalaisen kannettavaksi. Tällä on olennainen yhteys myös identiteettivarkauksiin.

6. Varmistamaton henkilöllisyys: Muukalaispassiin tai pakolaisen matkustusasiakirjaan mahdollisesti sisältyvä merkintä henkilöllisyyden varmistamattomuudesta ei näy lainkaan ajokortista. Näin ollen tällainen henkilö, jonka henkilöllisyyttä ei ole voitu varmistaa ja tästä on merkintä hänen matkustusasiakirjassaan, voi tieliikennesopimusten mukaan vaihtaa oman maansa ajokortin suomalaiseen. Hän voi käyttää ajokorttia asioinnissa tunnistamisasiakirjan tapaan, vaikka tosiasiassa hänen henkilöllisyyttään ei ole varmistettu.

7. Paperiset ulkomaiset ajokortit: Eräissä EU-maissa on edelleen laajassa tai jopa ainoassa käytössä paperinen ajokortti, johon on niitattu valokuva. Näitä maita ovat esimerkiksi Ranska ja Belgia. Lähtökohtaisesti ulkomaalaisella henkilöllä on maahan tullakseen oltava passi tai henkilökortti, joten ulkomaalaisen ajokortin käyttö on erityisen riskialtista missään tunnistamistarkoituksessa.

8. Ulkomaisen ajokortin vaihtaminen suomalaiseen: Ulkomaalainen henkilö saa Geneven ja Wienin tieliikennesopimusten mukaan vaihtaa ajokorttinsa suomalaiseen puolen vuoden maassa oleskelun jälkeen, mikäli haluaa ajaa Suomessa ilman uutta kuljettajatutkintoa. Lähes kaikki maat ovat liittyneet näihin tieliikennesopimuksiin. Tämän kohdan osalta ongelmana ei ole ajo-oikeus, vaan ajokortin käyttäminen tunnistamisasiakirjana.

   Erityisen ongelmallisia ovat ulkomaalaisille vaihdettavien suomalaisten ajokorttien luotettavuus. Vaihdetut ajokortit ovat fyysisesti täysin samanlaisia Suomessa alun perin myönnettyjen korttien kanssa ja vain viimeisin vaihtomaa näkyy kortin takana erityisehtokentässä maakoodina.

   Brysselissä kokoontuvan EU:n Fauxdoc/ Väärät asiakirjat -työryhmän agendalle on otettu matkustusasiakirjojen ohella myös ajokortit. Työryhmän 23.3.2009 järjestetyssä kokouksessa esitellyn kyselyn tulosten mukaan 84 % jäsenmaista on tavannut kolmansien maiden kansalaisille väärin perustein myönnettyjä ajokortteja. Jäsenmaista 78 % toivoo, että jatkossakin työryhmä käsittelisi asiaa. Kahdeksalla jäsenmaalla on suuria ongelmia ajokorttien vaihdon osalta, erityisesti Belgialla ja Ranskalla. Ranskassa on havaittu, että noin 22 - 30 % kolmansien maiden ajokorteista, joita pyritään vaihtamaan, ovat olleet vääriä tai väärennettyjä. Väärennöksien määrät ovat olleet kasvussa. Uhkana on, että annettaisiin petoksen tekijälle viranomaisen myöntämä aito asiakirja, jota voisi käyttää henkilötodistuksena Ranskassa. Belgiassa vastaavat luvut ovat myös 10 -15 %. Internetissä toimii esimerkiksi eräs palvelu, jonka avulla asiakas voi saada ostotuotteena useimpien maiden, myös Suomen, ajokortin ilman kokeita hyödyntäen eri maiden korttien vaihtokelpoisuutta.

9. Ajokorttien vaihtamisen ketjuttaminen: Väärinkäytöksen muotona esiintyy ulkomaisten ajokorttien vaihtamisen ketjuttamista, jolloin esimerkiksi kolmannen maan kortti vaihdetaan johonkin EU-maan korttiin ja tästä edelleen toisen EU-maan korttiin, jolloin kortissa näkyy viimeinen vaihtomaa, ei alkuperäistä myöntömaata. Kortti näyttää EU-ajokortista vaihdetulta, vaikka onkin alun perin Afrikassa myönnetty. Näiden ajokorttien ketjuttaminen voi aiheuttaa vakavan vaaran, mikäli niitä käytetään henkilöllisyyttä osoittavina asiakirjoina.

10. Poisottaminen: Ajokortti voidaan ottaa haltijaltaan pois tietyksi ajaksi tai kokonaan. Henkilöllisyyttä osoittavaa asiakirjaa ei voida ottaa rangaistuksen luonteisesti pois.

11. Ajokortin peruuttaminen: Mikäli ajokortti, passi tai henkilökortti varastetaan, keskeistä on asiakirjan poissaaminen tekijältä. Vaikka tekijä saataisiin kiinni tai hän olisi poliisin tiedossa, väärinkäytöstilanne ei välttämättä korjaannu, mikäli myös itse asiakirjaa ei saada pois tekijän hallusta. Katoamisilmoituksen voi tehdä poliisille, mutta palveluntarjoajat ja muut viranomaiset eivät saa tietoa ka-

donneesta tai anastetusta asiakirjasta, eikä ilmoitusta voi tehdä mihinkään yleisesti nähtävillä olevaan järjestelmään. Kansalaisen kannalta olisi hyvä, mikäli palveluntarjoajalla tai viranomaisella olisi mahdollisuus huomata tunnistamistilanteessa, että tunnistamisasiakirja onkin ilmoitettu varastetuksi tai kadonneeksi. Erityisen ongelmallinen tilanne on ajokortin osalta, koska mitään järjestelmää ei luotu ajo-oikeutta osoittavalle asiakirjalle. Kadonneeksi ilmoitettu passi ja henkilökortti on mahdollista Euroopan laajuisesti huomata rajanylitystilanteessa ja näiden asiakirjojen osalta poliisi ja rajavartiolaitos saavat tietokannasta tiedon asiakirjan kadottamisesta, mikäli henkilö on tämän ilmoituksen asianmukaisesti tehnyt.

4.3.3 Henkilökortti

Identiteettivarkauksien nopea lisääntyminen kansainvälisesti tekee osaltaan tarpeelliseksi tarkastella henkilökortin laajempaa käyttöä turvallisena tunnistamisasiakirjana. Jatkossa voisi olla mahdollista, että henkilökortti myönnettäisiin kansalaisen niin halutessa samalla kertaa kuin passi yhteismyöntöprosessina. Näin ollen poliisin tekemä tunnistamishinta perittäisiin vain kerran ja täten ainakin toisen asiakirjan hinta voisi madaltua. Tällä olisi myös merkitystä myös siksi, että ajokortin käytön vähentäminen tai kokonaan lopettaminen tunnistamisasiakirjana edellyttäisi jonkun muun kortin laajaa käyttämistä. Henkilökortti on valmis ja turvallinen tuote tunnistamiseen. Henkilökortit ovat matkustusasiakirjoja sekä henkilöllisyyttä osoittavia asiakirjoja. Biometristen tunnisteiden lisääminen myös henkilökorteille parantaisi entisestään niiden turvallisuutta. Tässä tarkastelussa henkilökortin ongelmana voidaan pitää nykyistä 48 euron hintaa. Toki merkitystä hintaan on myös sillä, mitä henkilökortti jatkossa sisältää. Jotta henkilökortti voisi olla todellinen vaihtoehto ajokortin sijaan, sen hinnan tulisikin olla mahdollisimman alhainen. Passeja myönnetään vuosittain puoli miljoonaa kappaletta, joten yhteismyöntöprosessin volyymit olisivat merkittäviä.

Nyt kun henkilökortti on siirtynyt Lissabonin sopimuksen myötä EU-sääntelyn alle, EU-kehityksen seuraaminen on erityisen keskeistä ja henkilökortin muita käyttömuotoja matkustusasiakirjan lisäksi vaikea ennakoida. Henkilökortin käyttöön henkilöllisyyden osoittamisessa Lissabonin sopimus ei vaikuta.

Henkilökorttialusta voi sisältää erilaisia toiminnallisuuksia ja kansallisia henkilökortin myöntökombinaatiomahdollisuuksia voi olla monia, esimerkiksi:

1. Sirullinen henkilökortti, jossa kansalaisvarmenne (nykyinen versio)
2. Sirullinen henkilökortti, jossa biometriset tunnisteet
3. Kahden sirun henkilökortti, jossa kansalaisvarmenne sekä biometriset tunnisteet
4. Siruton henkilökortti ilman kansalaisvarmennetta tai biometrisia tunnisteita
5. Siruton kortti ja lisäksi tarjolla sirullinen henkilökortti, jossa kansalaisvarmenne
6. Siruton kortti ja lisäksi tarjolla sirullinen biometriset tunnisteet sisältävä henkilökortti.

7. Siruton kortti ja lisäksi kahden sirun henkilökortti, joka sisältäisi kansalaisvarmenteen ja biometriset tunnisteet
8. Vaihtoehdot 1-8 ja lisäksi muita toiminnallisuuksia esim. matkakortti

   Erilaiset sirujen toiminnallisuudet ja myöntökombinaatiot määrittelee aina voimassaoleva lainsäädäntö sekä myöntöprosessin sekä korttien taloudelliset vaikutukset, jotka määritellään aina ennen korttien hankintamenettelyä.

4.4 Kansalaisvarmenne ja tulevaisuuden käyttömuodot

4.4.1 Yleistä

Sisäasiainministeriö katsoo, että valtiollinen henkilöllisyyden vahvistaminen ei tulisi rajoittua vain fyysisiin dokumentteihin, passiin ja henkilökorttiin, vaan valtion vahvistama perusidentiteetti olisi kyettävä vahvistamaan myös verkossa. Lainsäädäntö mahdollistaa tälle jo nykyisin tältä osin monta eri alustaa.

Sisäasiainministeriö katsoo, että valtion verkossa vahvistamasta perusidentiteetistä luopuminen on yhtä kuin kysymys valtion ydintehtävien määrittelystä liittyen kansalaisen oikeuteen henkilöllisyydestä. Luotettavan henkilöllisyyden varmistaminen ja takaaminen on valtion ydintehtävä. Kansalaisella on oikeus henkilöllisyyteen, eikä kysymystä voida tarkastella yksinomaan taloudellisena kysymyksenä. Henkilöllisyysvarkauksien ennaltaehkäisyn kannalta luotettava tunnistaminen on ensiarvoisen tärkeää. Mikäli kansalaisvarmenteesta luovutaan kokonaan, valtion tehtäviin jäisi vain fyysisten (passi ja henkilökortti) henkilöllisyyttä osoittavien asiakirjojen myöntäminen. Valtio ei enää jatkaisi kansalaisten henkilöllisyyden varmistamista lainkaan verkossa. Henkilöllisyyden varmentaminen sähköisessä toimintaympäristössä tulee kuitenkin olemaan jopa fyysisiä henkilöllisyystodistuksia tärkeämpää asioinnin ja palveluiden siirtyessä enenevässä määrin vain verkkoon. Perustuslain 6 §:ssä säädetään kansalaisten yhdenvertaisuudesta. Luotettavaa sähköistä tunnistamista voidaan pitää tietoyhteiskunnan peruspalveluna ja kansalaisten yhdenvertaisuus edellyttää, että kansalaisella on mahdollisuus saada luotettava sähköinen tunnistusväline. Valtion takaama varmenne turvaa kansalaiselle yhdenvertaiset mahdollisuudet asioida sähköisesti. Kun julkinen hallinto enenemässä määrin hakee tuottavuutta lisäämällä sähköisiä palveluita, on kyseenalaista, että henkilöllä on oltava sopimussuhde yksityisen palveluntarjoajan kanssa voidakseen käyttää julkisen hallinnon tarjoamia sähköisiä palveluita. Tietoyhteiskunnan ydintehtäviin voidaan katsoa kuuluvan, että se tarjoaa turvallisen sähköisen asioinnin ja kehittyneen sähköisen allekirjoituksen luontivälineen. Lähivuosina tulevat verkossa tapahtuvat oikeustoimet lisääntymään. Jos valtio ei enää myönnä kansalaisvarmennetta, kansalaisilla ei ole tulevaisuudessa mahdollista tehdä sähköisistä allekirjoituksista annetun lain mukaista kiistämätöntä allekirjoitusta. Tätä voidaan pitää tietoyhteiskunnassa selvänä puutteena.

Sisäasiainministeriö katsoo, että kansalaisten asiointipalveluiden takaamisen kannalta on olennaista, että kansalaisille voidaan tarjota taloudellisista ryhmittymistä riippumaton, neutraali ja riittävän turvallinen asiointiväline, jonka käyttö verkkopalveluissa on maksutonta. Tällä hetkellä esimerkiksi markkinoilla olevilla pankkitunnisteilla tehdään määrällisesti runsaasti transaktioita. Sähköisen asioinnin kytkeminen pelkästään pankin asiakkuuksiin on ongelmallinen erityisesti sellaisten henkilöiden kohdalla, joilla on luottotiedoissa merkintä ja pankkitunnusten saaminen sähköiseen asiointiin voi olla mahdotonta. Lisäksi pankkien tuottamat tunnistuspalvelut ovat käytännössä hyvin kalliita julkishallinnon palveluiden tuottajille.

Poliisi lisäsi sähköiseen rikosilmoitukseen sähköisen tunnistamisen heinäkuussa 2009. Asiasta käytiin heinäkuussa vilkasta kansalaiskeskustelua verkossa. Kansalaiskeskustelussa kansalaiset ovat nimenomaan viitanneet julkisen hallinnon ja julkisen vallankäytön riippumattomuuteen ja neutraaliuteen. Kansalaisten yhdenvertaisuuteen ja tasapuoliseen kohteluun kuuluu se, että julkisten palvelujen käyttäminen tulee olla mahdollista neutraalilla tavalla ilman edellytystä kuulua jonkun yksityisen tahon asiakkaaksi.

4.4.2 Tulevaisuuden käyttömuodot

Eräs vaihtoehto kansalaisvarmenteen alustasta on USB-tikku. Tätä mahdollisuutta on esiselvitetty Väestörekisterikeskuksen johdolla ja lähtökohtaisesti tämä olisi teknisesti mahdollista. USB-tikku olisi mahdollista myös myöntää henkilökortin tapaan yhdessä passin tai henkilökortin kanssa yhteismyöntöprosessissa.

Riippuen mikä VM:n varmennetuotannon uudelleen organisointia pohtivan työryhmän vaihtoehdoista valitaan sekä miten EU-lainsäädäntö kehittyy, kansalaisvarmenteen tulevaisuudelle on monta eri vaihtoehtoa. Itse henkilökortin olemassaoloon kansalaisvarmenteeseen mahdollisesti tehtävät muutokset eivät ole vaikuta.

4.4.3 Kansainvälinen kehitys

Valtaosalla eurooppalaisista valtioista on joko käytössä tai on valmisteilla vastaavanlainen valtion takaama, taloudellisista yhteenliittymistä neutraali sähköinen henkilökortti. European eGovernment Services (IDABC) esitti eurooppalaisesta tilanteesta vuonna 2008 seuraavaa: 28 maata 32:sta (87,5 %) käyttävät tai suunnittelevat käyttöönsä varmenteeseen liittyviä sähköisiä henkilöllisyyksiä. 22 maata 32:sta (68 %) on implementoinut varmenteen käyttöön perustuvia palveluita hallinnon palveluihin liittyen, vain seitsemän maata ei raportoinut erityisistä sähköisistä hallintopalveluista. 84 % jäsenvaltioista eli 27 valtiolla on jo käytössä henkilökortti, 7 valtiota rakentavat järjestelmää parhaillaan ja 14 valtiota ovat suunnittelemassa lähiaikoina tuotettavaa henkilökorttia. 75 % jäsenvaltioista on rakentanut tunnistautumisjärjestelmänsä perustuen PKI -varmenteisiin.

Euroopan komissio on 29.11.2008 julkistamassaan Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market -asiakirjassaan (COM(2008) 798 lopullinen) julkistanut sähköisistä allekirjoituksista annetun direktiivin 1999/93/EY seurantaan ja toteutumisen liittyvät toimenpiteet. Palveludirektiivin 2006/1223/EY mukaisesti vuoden loppuun mennessä asiointipalvelut on voitava toteuttaa koko prosessin osalta sähköisesti. Edellä mainitussa Action Planissa on esitetty seuraavia sähköiseen allekirjoitukseen liittyviä vaatimuksia ja edellytyksiä.

Yli jäsenvaltioiden rajojen toimivien luottamusketjujen rakentaminen on Euroopan komission näkemyksen mukaisesti yksi tekijä, joka helpottaa laatuvarmenteella tehtyjen allekirjoitusten leviämistä ja sitä kautta palvelujen saatavuutta. Action Planissa on kuvattu komission analyysi toimenpiteistä, jonka mukaiset tehtävät jakaantuivat vuoden 2009 eri neljänneksille. Komissio on kiinnittänyt samassa asiakirjassa huomiota myös sähköisen identiteetin hallintajärjestelmän luomiseen tavoitteenaan luoda yhdenmukainen eurooppalainen identiteetti. Yksi ilmaus tästä pyrkimyksestä on STORK-ohjelma, jonka piloteissa myös Suomi on mukana.

Euroopan unionissa on keskeiseksi asiaksi noussut henkilön luotettava tunnistaminen. Tämä on tärkeä turvallisuuskysymys kansallisvaltioille. Luotettava henkilöllisyyden todentaminen on tärkeää myös sen vuoksi, että niihin liittyvät väärinkäytökset ovat selvitysten valossa usein osa muuta laajempaa järjestäytynyttä rikollista toimintaa kuten esimerkiksi rahanpesua ja terrorismin rahoittamista.

Ohessa on listattu esimerkkejä hallinnon palveluista, joissa Euroopan komission IDABC:n verkkosivuillaan julkaiseman tutkimuksen mukaisesti käytetään laatuvarmenteeseen perustuvaa allekirjoitusta. Tällaisia ovat veropalvelut (Itävalta, Belgia, Slovakia, Ruotsi, Espanja), äänestäminen (Viro), posti- ja logistiikkapalvelut (Itävalta, Saksa) sekä yrityspalvelut (Itävalta, Portugali, Ruotsi). Laatuvarmenteita käytettiin muun muassa seuraavan tyyppisissä palveluissa: hankinta-asiat (Bulgaria, Alankomaat, Romania), veropalvelut (Bulgaria, Kroatia, Tshekki, Slovenia, Alankomaat), eläke- ja sosiaalipalvelut (Bulgaria, Kroatia, Unkari, Slovenia) ympäristöön ja maatalouteen liittyvät palvelut (Slovenia) sekä kansalliset hallinnon portaalit (Bulgaria, Unkari).

EU:ssa on ollut suunnitteilla Eurooppalaisen kansalaiskortin (European Citizen Card) käyttöönotto. Kyseessä on ensimmäinen eurooppalainen sähköiselle hallinnolle tarkoitettu standardointiratkaisu, jossa käytetään kortille räätälöityjä standardiprofiileja. Eurooppalainen kansalaiskortti on yhteensopiva erilaisten henkilöllisyyden hallintajärjestelmien kanssa, painoarvoa on annettu yksityisyydelle ja käytettävyydelle ja yhteistyötä on ehdotettu myös Eurooppalaisen sähköisen terveysvakuutuskortin kehittämistahoille.

Eurooppalaisen kansalaiskortti -standardin (European Citizen Card) suhteen ei ole vielä ryhdytty biometriikkatyöhön, mutta yhteistyötä tehdään CEN Focus Groupin (The European Committee for Standardization (CEN)) asiantuntijoiden kanssa. Eurooppalaista

kansalaiskorttia on valmisteltu pitkään, mutta sen tarkemmasta aikataulusta ole tässä vaiheessa vahvistettua tietoa.

4.5 Identiteettivarkauksien torjunta

Identiteettivarkauksilla voidaan loukata useita eri perusoikeuksia, kuten oikeutta yksityiselämän ja omaisuuden suojaan. Siksi yhteiskunnan tulisi suojella henkilöitä identiteettivarkauksilta tai ainakin niiden vaikutuksilta. Vaikutuksia voidaan rajata tehostamalla ennaltaehkäisyä ja toipumista, mutta myös tarkastelemalla sitä, ovatko rikosoikeudelliset keinot ajan tasalla maailman muuttuessa.

Perinteisten tekojen osalta ei ole nähtävissä sellaisia ongelmia, joiden ratkaisemiseksi tarvittaisiin rikosoikeudellista tarkastelua. Oikeusministeriö toteaa lausunnossaan Valtioneuvoston periaatepäätökseen sähköisestä tunnistamisesta: (luku 2.6.2): ”Toisen henkilötietojen väärinkäyttö on jo nyt rangaistavaa teon luonteesta riippuen petoksena, maksuvälinepetoksena, väärennyksenä, henkilörekisteririkoksena, rekisterimerkintärikoksena, väärän todistuksen antamisena viranomaiselle, väärän henkilötiedon antamisena, vahingontekona, luvattomana käyttönä, tietojärjestelmän häirintänä jne. Lisäksi jo maksuvälinepetoksen valmistelu on säädetty erikseen rangaistavaksi (RL 37:11). ”

Sen sijaan tietoverkossa tilanne on toinen. Verkossa rikosvahingon kokonaispotentiaali on suurempi samaan aikaan kun tutkinnan toimivaltuudet ovat varsin olennaisesti reaalimaailmaa heikommat. Silti verkonkin osalta tarvitaan myös muita kuin rikosoikeudellisia keinoja erityisesti rikosten ennaltaehkäisyn tehostamiseksi. Muidenkin keinojen on kuitenkin oltava tasapainossa saavutettavan hyödyn kanssa.

Jotta perusoikeudet voivat konkreettisesti toteutua, myös lainsäädännön olisi otettava huomioon ympäristön erityiset ominaispiirteet myös silloin kun ympäristö olennaisesti muuttuu. Fyysinen ja sähköinen toimintaympäristö eroavat toisistaan monin eri tavoin, etenkin tiedon levittämis- ja yhdistämismahdollisuuden osalta. Verkkoympäristö on kansalaiselle hankala ja riskien tunnistaminen on vaikeaa. Verkkoympäristöön kenelläkään ei ole täydellistä kontrollia, koska kyse on myös kansainvälisestä toimintaympäristöstä.

Rikosoikeutta ja pakkokeinoja on kuitenkin aina pidettävä ongelman ratkaisun viimesijaisina keinoina. Näin ollen myös kevyempiä vaihtoehtoja on syytä aina harkita, vaikka verkkoympäristö onkin tässä suhteessa erityisen haasteellinen. Rikosoikeuden, pakkokeinojen, toimivaltuuksien ja kevyempien keinojen yhdistelmä onkin kattavin ratkaisu ja näistä kaikista osista koostuva strateginen suunnitelma identiteettivarkauksien torjuntaan on myös tarpeen. Tällainen suunnitelma löytyy muun muassa Yhdysvalloista vuodelta 2007.[4]

[4] Strategic Plan: www.idtheft.gov

Tällainen suunnitelma muodostuu seuraavista osa-alueista:

1. Ennaltaehkäisy: henkilötietojen ja identiteettitietovälineiden saannin rajoittaminen
    a) Rajoitetaan henkilötietojen yleistä ja erityistä saatavuutta[5]: Henkilötunnuksen suojaaminen, luottokorttitietojen säilyttäminen ja suojaaminen sekä tunnistamisasiakirjojen turvatekijät ja tunnistaminen.
    b) Suojataan henkilötietovarastoja
    c) Kansalaisten valistaminen omasta vastuusta

2. Väärinkäytösten ehkäisy: vaikeutetaan toisen henkilötietojen käyttämistä
    a) Riittävän tunnistamisen tason valinta
    b) Muiden tunnistusrutiinien kehittäminen: esim. turvakysely siten, ettei tietojärjestelmä avaudu vain henkilötunnuksella
    c) Kansalaisten toimenpiteet väärinkäytösuhan kasvaessa (esimerkiksi lompakko varastetaan): passi- ja ajokorttirekisterin merkinnät ja tiedon välitys eteenpäin (erityinen sulkulistapalvelu)

3. Pakkokeinot ja rikostutkinta
    a) Julkaistavat varoitukset ja epäilyttävän tietoliikenteen sulkeminen
    b) Laittomasti kerätyn henkilötietoaineiston takavarikointi
    c) Rikostutkinta rajat ylittävässä verkkorikollisuudessa

4. Identiteettivarkauksista palautuminen
    a) Rikoksen kohteen kannalta
    b) Tiedon kohteen kannalta

5. Henkilötietojen luvattoman käytön kriminalisointi
    a) Missä määrin luvaton käyttö tulee rangaistavaksi muiden tunnusmerkistöjen yhteydessä?
    b) Miltä osin tarvittaisiin uutta kriminalisointia ja mitä lisäarvoa se toisi?

4.5.1 Muut kuin rikosoikeudelliset torjuntakeinot

4.5.1.1 Perinteisten tekojen vaikutusten rajaaminen

Perinteisten, reaalimaailmassa tapahtuvien tekojen osalta on nähtävissä kaksi erityistä toimintaprosesseihin liittyvää haavoittuvuutta, jotka mahdollistavat osaltaan taloudellista hyötyä tavoittelevien rikosten toteuttamisen ja ovat tulleet myös esimerkkitapauksissa esille: ajokortin käyttö tunnistamisasiakirjana sekä osoitteenmuutoksen tekeminen puhelimella ilman luotettavaa vahvaa tunnistamista.

---

[5] Tietojen saannin rajoittaminen tietyistä rekistereistä väärinkäytösten estämiseksi ja rikosturvallisuuden parantamiseksi. Sisäasianministeriön julkaisuja 49/2007

Perinteisten identiteettivarkauksien vaikutusten rajaamiseksi tulisi huomio kiinnittää uhrin aseman parantamiseen identiteettivarkauden tapahduttua. Se, jonka nimissä rikos tehdään, joutuu näkemään kohtuuttomasti vaivaa perintäliiketoiminnan ja palveluntarjoajien kanssa. Yhteiskunnan tulisi voida tarjota uhrille yksinkertaisempi menettely vahingoilta suojautumiseen. Eräs ratkaisu voisi olla keskitetty ilmoitusjärjestelmä. Identiteettivarkauden uhriksi joutunut henkilö voisi ilmoittaa yhteen paikkaan tekemästään rikosilmoituksesta ja tästä järjestelmästä tieto leviäisi eteenpäin. Tilanne on nyt kohtuuton, koska näyttää siltä, että aiheettomien perintäkirjeiden tuloa ei uhri voi käytännössä estää.

4.5.1.2 Tietoverkossa toteutettujen tekojen ennaltaehkäisy

Taloudellista hyötyä tavoittelevan ammattimaisesti toteutetun identiteettirikollisuuden tekee poikkeuksellisen kannattavaksi sen toteuttamisen kustannustehokkuus sekä pieni kiinnijäännin riski. Rikostorjunnallista hyötyä saadaan tällöin vaikuttamalla ennaltaehkäisevästi mihin tahansa rikollista liiketoimintaa edesauttavista tekijöistä. Koska viranomaisten toimivaltuudet eivät aina kaikilta osin tue rikosten menestyksellistä tutkintaa, eräs rikostorjunnan keino tulee lähitulevaisuudessakin olemaan rikosten liiketoimintamallin tunnistaminen ja toteuttamisen vaikeuttaminen. Rikoksen toteutuskustannuksia voidaan kasvattaa parantamalla olennaisesti yleistä tietoturvatilannetta, mihin tarvitaan lukuisten yksityisten ja julkishallinnon toimijoiden yhteistyötä.

Taloudellista hyötyä tavoittelevien identiteettirikosten uhka ei tulevaisuudessa kohdistune ensisijaisesti palveluntarjoajiin, vaan asiakkaisiin, joiden käyttämien laitteiden tietoturvallisuus on lähes kokonaan palveluiden tarjoajien ulottumattomissa. Palvelun suunnittelussa tehdyillä valinnoilla ja palveluprosessilla voidaan kuitenkin vaikuttaa olennaisesti palvelun turvallisuuteen, mistä Suomen tilanne onkin hyvä esimerkki. Suomessa tietoturvallisuus on alusta asti huomioitu suunnittelussa ja henkilötietojen käsittelyä säätelevää lainsäädäntöä on systemaattisesti jalkautettu palveluiden tarjoajien helposti ymmärtämään muotoon. Muualla maailmassa jo pelkästään phishingin vahingot ovat olleet mittavia, mutta Suomessa alle 100 000 € (olkoonkin, että juuri phishingiltä meitä suojelee myös sopivan outo kielemme). Tulevaisuus ei kuitenkaan näytä yhtä valoisalta: muun maailman suojausten parantuessa Suomen tasolle, rikolliset kehittävät menetelmiä, jotka alkavat toimia myös täällä.

Erilaisten huijausten onnistumiseen käyttäjä voi vaikuttaa omalla toiminnallaan. Kuluttajilta kysellään yhä useammin internetissä ja sähköpostissa heidän identiteettinsä kannalta keskeisiä tietoja. Muun muassa Kuluttajavirasto, tietosuojavaltuutetun toimisto ja Viestintävirasto useasti tiedottaneet, että kaikkiin tunnistetietojen pyyntöihin on syytä suhtautua varauksella. Tietoja on säilytettävä samalla huolellisuudella kuin käteistä rahaa, pankkikorttia ja luottokorttia. Niitä ei pidä paljastaa tuntemattomille tahoille, ellei voi olla varma niiden turvallisesta käsittelystä.

Sen sijaan käyttäjän mahdollisuudet torjua tietoteknistä tiedonkaappaamista ovat paljon rajallisemmat. Kuluttajien yleisimmissä käyttöympäristöissä käyttäjällä ei ole riittäviä edellytyksiä havaita tietojensa kaappaamista. Haavoittuvan koneen tartuttaminen tietoa kaappaavalla haittaohjelmalla ei enää edellytä vierailua sen enempää epämääräisellä www-sivulla kuin muutakaan erityistä huolimattomuutta – muutoin kuin koneen päivittämisen suhteen. Palveluntarjoajat ja tietoturvayhteisö (mm. Viestintäviraston CERT-FI -yksikkö ja tietoturvateollisuus) tekevät tällä hetkellä erinomaista työtä pohtiessaan keinoja kuluttajan suojaamiseksi, mutta lopulta ongelma on rakenteellinen.

Ohjelmistovalmistajilla ei ole välttämättä riittävää kannustinta parantaa ohjelmistolaatua, ennen kuin kuluttajat sitä ehdottomasti vaativat. Siihen taas ei välttämättä ole riittävää intressiä ennen kuin vahingot realisoituvat kaikkien verkon toimijoiden osalta. Ohjelmistovalmistajille tulisi luoda kannustimia parantaa ohjelmistojen laatua, joskin kannustinten tulisi olla Euroopan laajuisia, jotta Suomen kilpailuasetelmaa ei vaikeuteta.

Tietoturvatietoisuuden parantamista on yhä syytä jatkaa. Käyttäjiä voisi muun muassa kehottaa hoitamaan verkkokauppa-, verkkopankki- ja viranomaisasioinnin eri laitteelta kuin muun verkkoviestinnän ja -selailun.

Jotta vahingot voidaan rajata mahdollisimman pieniksi, identiteettitietojen kaappauksesta on saatava mahdollisimman nopeasti tieto toimijoille. Eräänä mahdollisena keinona työryhmässä nousi esiin kotimaisen palveluntarjoajan informointivelvollisuus tietosuojavaltuutetun toimistolle havaitsemastaan henkilötiedon kaappaamisesta samaan tapaan kuin teleyrityksillä on sähköisen viestinnän tietosuojalain nojalla informointivelvollisuus Viestintävirastolle keskeisten tietoturvaloukkausten osalta. Jatkovalmistelussa tulisi kuitenkin suorittaa huolellinen intressipunninta, jotta yksityisille toimijoille ei synny velvoitteita, joista ei ole riittävää hyötyä. Identiteettitiedon kaappausta kun tapahtuu tällä hetkellä paljon asiakaspäästä, joka ei ole palveluntarjoajien toimivallan piirissä.

Ilmoitusvelvollisuus on ajankohtainen myös EU-tasolla. Lähitulevaisuudessa lieneekin syytä tarkastella identiteettitietojen kaappausta koskevaan tietoon kohdistuvia ilmoituksia yhtenä keinona rajata identiteettivarkauksista aiheutuvia vahinkoja. Komissio on ilmoittanut 4.11.2010 antamassaan tiedonannossa "Kattava lähestymistapa henkilötietojen suojaan Euroopan unionissa" (KOM (2010) 609 lopullinen) tutkivansa, voitaisiinko yleisessä säädöskehyksessä ottaa käyttöön henkilötietosuojan loukkausta koskeva yleinen ilmoitusvelvollisuus, jota varten määriteltäisiin, kenelle tällainen ilmoitus olisi osoitettava ja millä perusteella ilmoitusvelvollisuus syntyisi.

4.5.2 Kriminalisointiin ja viranomaistoimivaltuuksiin liittyviä kysymyksiä

4.5.2.1 Euroopan unionin ajankohtainen identiteettivarkaustarkastelu

Euroopan komission toimintasuunnitelmassa Tukholman ohjelman toteuttamiseksi KOM(2010) 171 lopullinen todetaan, että tietoverkkorikollisuutta olisi torjuttava kokonaisvaltaisella tavalla. Asiakirjassa todetaan, että komissio vastuutahona toteuttaa identiteetin hallintaa koskevan eurooppalaisen strategian sekä säädösehdotukset identiteettivarkauden kriminalisoinnista, sähköisestä identiteetistä ja suojatuista tunnistusjärjestelmistä.[6] Aikatauluksi on merkitty vuosi 2012.

Neuvoston puitepäätöstä 2005/222/YOS tietojärjestelmin kohdistuvista hyökkäyksistä (24.2.2005) ollaan muuttamassa. Uusi tietoverkkorikosdirektiiviehdotus, ehdotus Euroopan parlamentin ja neuvoston direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta, KOM (2010) 517 lopullinen, on ollut käsittelyssä EU-kokoustasolla. Direktiiviehdotuksessa esitetään verkkorikoksen kvalifiointiperusteeksi tilannetta, jossa verkkorikos toteutetaan väärällä identiteetillä siten, että identiteetin oikealle haltijalle aiheutuu vahinkoa.

Lisäksi EU-tasolla tehdään päätelmiä ja suosituksia identiteettipetosten osalta. Neuvoston päätelmät identiteettipetosten ehkäisemisestä ja identiteettihallinnosta mukaan lukien pysyvän strukturoidun yhteistyön kehittäminen jäsenvaltioiden välillä on hyväksytty 2-3.12.2010 OSA-neuvostossa. Etenkin uhrin avustamista koordinoidun yhteistyön avulla pidetään tärkeänä. Lisäksi luonnoksessa tuetaan jäsenvaltioiden pyrkimyksiä vahvistaa henkilötunnistamisprosessejaan, vaihtaa tietoja varastetuista henkilöllisyystodistuksista ja rohkaistaan aloitteita estää identiteettipetoksia.

4.5.2.2 Kriminalisointikysymyksiä taloudellisen hyödyn ID-rikoksissa

Uudemmat tietojen kaappausten tekotavat eivät ole rangaistavia johtuen kansallisen lainsäädännön muotoilusta. Verkkoteknologian ja tunnistamisen prosessien kehittymisen voidaan katsoa tältä osin ajaneen ohi lainsäädännön. Laillisuusperiaatteen nojalla rikosprosessissa ei voida tulkita lainsäädäntöä vastoin lain kirjainta, vaikka vaihtoehtoinen tulkinta joissakin tapauksissa selvästi noudattaisi lainsäätäjän tarkoitusta.

Rikoslain 38 luvun 3 § viestintäsalaisuuden loukkaus suojaa ainoastaan verkossa kuljetettavana olevaa tai tietojärjestelmään suojatusti tallennettua viestiä. Nykyisissä tekota-

[6] Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Vapauden, turvallisuuden ja oikeuden alueen toteuttaminen EU:n kansalaisten hyväksi. Toimintasuunnitelma Tukholman ohjelman toteuttamiseksi. Bryssel 20.4.2010. KOM(2010) 171 lopullinen.

voissa tietoa ei kuitenkaan kaapata ”langalta” tai talletetusta ja suojatusta tiedostosta, vaan järjestelmän sisäisestä käsittelystä esimerkiksi näppäinpainalluksia kaappaamalla. Kansallinen pykälä ei näin täytä kokonaisuudessaan Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen määritelmää, jossa myös tiedon kaappaaminen tietojärjestelmän sisältä on esitetty rangaistavaksi. Myöskään vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9a) ei kata tällaisen haitallisen ohjelman käyttämistä tarkoituksena hankkia tietoa oikeudetta. Haittaohjelmien käyttämistä ei ylipäätään ole kriminalisoitu, vaan hiukan vanhahtavasti lähinnä niiden levittäminen. Nykyisin kuitenkin levitysvaihe ja tiedon keruu tapahtuvat yleensä erikseen. Nykyinen kansallinen lainsäädäntö ei anna viranomaisille toimivaltuutta puuttua luottamuksellisen tiedon kaappaamiseen, milloin kaappaaminen tapahtuu asiakaspään työasemasta asioinnin yhteydessä. Eräissä tapauksissa henkilörekisteririkos tai maksuvälinepetoksen valmistelu saattavat täyttyä, mutta niiden täyttyessä poliisilla taas ei ole toimivaltuutta tutkia rikosta verkossa (avattu seuraavassa luvussa 4.5.2.3).

4.5.2.3 Toimivaltuuksista taloudellista hyötyä tavoittelevissa ID-rikoksissa

Tietoverkossa tilanne on olennaisesti erilainen kuin reaalimaailmassa, sillä tietoverkossa rikoksesta ei ole olemassa juuri muita jälkiä kuin tietoteknisiä lokijälkiä ja niiden käyttämisen kynnys on paljon reaalimaailmaa korkeampi: Reaalimaailmassa kirjeen sisällön ja osoite- ja lähetystiedot voi tutkia, jos epäillään rikosta, josta saatava ankarin rangaistus on vähintään vuosi vankeutta. Tietoverkossa tunnistamistiedot voi voimassaolevan lainsäädännön puitteissa tutkia tuomioistuimen määräämän televalvontaluvan perusteella, jos epäillään rikosta josta säädetty ankarin rangaistus on neljä vuotta vankeutta. Haittaohjelmaliikenteenkin sisältö on mahdollista tutkia vain erikseen nimetyissä vakavissa rikosnimikkeissä, kuten tutkittaessa esimerkiksi henkirikosta, törkeää kiristystä tai törkeää vahingontekoa.

Identiteettitiedon oikeudetonta keräämistä ei ole tiedon keruuvaiheessa yleensä mahdollista tutkia eikä tulevaa vahinkoa estää, jos keruu tapahtuu tietoverkossa. Niinpä viranomainen ei voi käynnistää välttämättömiä tutkintatoimenpiteitä siinä vaiheessa, kun tietotekninen jälki olisi vielä saatavilla. Kuten edellä luvussa 4.5.2.2 tuotiin esiin, keruu on osittain kriminalisoitu, mutta sellaisella rikosnimikkeellä, joka ei mahdollista tietoverkossa välttämättömien telepakkokeinojen käyttöä. Kyseeseen tulee lähinnä henkilörekisteririkos (RL 38:9), maksuvälinepetoksen valmistelu (RL 37:11) tai petos (RL 36:1), joiden tutkinnassa ei voida käyttää telepakkokeinoja yhteydentarjoajan hallussa olevien lokijälkien selvittämiseksi. Koska tällaisissa rikoksissa petos kohdistuu ihmiseen eli käyttäjään, eikä tietojärjestelmään, televalvonnan (PKL 5a:3) 1 momentin 2 kohdan alhaisempaa kynnystä[7] ei voida soveltaa.

[7] Pakkokeinolain 5a luvun 3 § 1 momentin 2) automaattiseen tietojenkäsittelyjärjestelmään *kohdistuneesta* rikoksesta, joka on tehty telepäätelaitetta käyttäen

Esitutkintaviranomaisella on sen sijaan oikeus tutkia vanhemmilla tekotavoilla toteutettuja palvelinmurtoja, sillä lainsäätäjä on kaukaa viisaasti jo 1990-luvulla tunnistanut sen, ettei tietoverkossa ole muita silminnäkijähavaintoja kuin tietotekniset lokijäljet. Niinpä televalvonnan kynnystä on pakkokeinolain 5a luvussa alennettu ” 2) automaattiseen tietojenkäsittelyjärjestelmään kohdistuneesta rikoksesta, joka on tehty telepäätelaitetta käyttäen.” Ympäristö on sittemmin kuitenkin muuttunut. Tiedon kaappaukseen ei enää välttämättä liity ”hakkerointikomponenttia” tai hakkerointi tehdään erillisenä tekona, tiedon kaappaaminen toisena. Niinpä aiemmin hyvin toiminut poikkeus ei enää kata koko kenttää.

Identiteettitiedon oikeudeton käyttäminen taloudellisen hyödyn hankkimiseksi on lähes aina kriminalisoitu. Rikosnimikkeinä kyseeseen tulevat usein (törkeä) maksuvälinepetos, (törkeä) petos, (törkeä) rahanpesu ja kätkentä sekä laittoman maahantulon järjestäminen. Esitutkintaviranomaisilla on rikosnimikkeiden täyttyessä hyvät toimivaltuudet selvittää viestinnän tunnistamistiedot. Tietoverkossa rikoksen tutkiminen on tiedon väärinkäyttöön liittyvien tunnusmerkistöjen täyttyessä kuitenkin käytännössä liian myöhäistä, sillä tiedon keräämiseen liittyvä tietotekninen jälki ei enää ole tallella.

Tietoverkossa viestintä- tai liikennöintiyhteydestä syntyvä tietotekninen jälki on olemassa vain varsin lyhyen ajan, koska palveluntarjoajilla ei ole liiketoimintaintressiä säilyttää tietoa. Mahdollinen tietotekninen jälki on olemassa vain hetken sen jälkeen, kun tietoa kaapataan. Siinä vaiheessa, kun kaapattua identiteettitietoa käytetään myöhemmin väärin, alkuperäisen tietokaappauksen jälkeä ei enää ole olemassa. Identiteettitiedon kaappaamisen kriminalisoinnille ei ole nähty aiemmin tarvetta, koska tunnistetiedon oikeudeton käyttäminen yleensä täyttää jonkin rikostunnusmerkistön. Reaalimaailmassa teko onkin usein selvitettävissä vielä tässä vaiheessa. Tietoverkko on kuitenkin muuttanut tilannetta, koska verkossa voidaan melko helposti kerätä tietoa sadoilta tuhansilta asianomistajilta ilman, että jälki teosta säilyisi.

Tietoverkossa toteutetun rikoksen tutkinnassa keskeinen toimivaltaongelma aiheutuu siitä, ettei rikoksentekijän jäljittäminen ole lähtökohtaisesti mahdollista ilman tietoverkon lokitietojen käsittelyä. Ne taas eivät ole esitutkintaviranomaisen käytettävissä ilman telepakkokeinojen (pakkokeinolain 5a luku) edellytysten täyttymistä. Viestinnän tunnistamistietojen hankkimisesta esitutkintaa varten päättää tuomioistuin joko pakkokeinolain televalvonnan (PKL 5a:3) tai sananvapauden käyttämisestä joukkoviestinnässä annetun lain (460/2003, jäljempänä sananvapauslaki) 5 luvun 17 §:ssä tarkoitettujen verkkoviestin tunnistamistietojen luovuttamista koskevien edellytysten täyttyessä. Kynnys on varsin korkea. Eräin poikkeuksin tunnistamistiedot voi hankkia viestistä tutkittaessa rikosta, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta. Telepakkokeinojen korkean kynnyksen ja tuomioistuimelle säädetyn päätäntävallan tavoitteena on turvata perustuslain tasoista suojaa nauttivaa luottamukselliseksi tarkoitettua viestintää (PL 2:10) erityisesti rikoksesta epäillyn osalta. Telepakkokeinot on kuitenkin suunniteltu suljettuun televerkkoon, jossa osapuolet ovat pääsääntöisesti asiakassuhteessa palveluntarjoajaan ja siten tunnistettavissa ja jossa kaikki liikenne on henkilöiden väli-

tä viestintää. Kumpikaan lähtöoletus ei välttämättä täyty avoimessa tietoverkossa. Jos verkko-osoitteen käyttäjä ei ole asiakassuhteessa palveluntarjoajaan, epäillyn henkilöllisyys ei selviä verkko-osoitteen selvittämisen avulla. Tällöin tuloksena on tilanne, jossa abstrakti verkkoidentiteetti nauttii yhteiskunnan taholta suurempaa suojaa kuin rikoksen uhriksi joutunut todellinen henkilö.

Vaikka tiedon käyttö olisi kriminalisoitu, viranomaisen toimivaltuudet eivät silti ole aina riittävät tutkintaan. Maksukorttirikollisuudessa kasvava ilmiö on ”low value, high volume”-teot, joissa suureksi muodostuva rikoshyöty kostuu valtavasta määrästä yksittäisiä pienehköjä vahinkoja. Tietoa käyttäessä täyttyy tällöin vain petostunnusmerkistö, jolloin telepakkokeinojen käyttö ei silti ole mahdollista yksittäisen teon tutkinnassa. Törkeän maksuvälinepetoksen (RL 37:9) tai törkeän petoksen (RL 36:2) tutkinnassa olisi mahdollista käyttää televalvontaa, mutta yksittäiset tapaukset toteutetaan tarkasti siten, että ne täyttävät vain perusmuotoisen tai lievän maksuvälinepetoksen (RL 38:8, RL 38:10). Kvalifiointiperusteen tunnistaminen edellyttäisi yksittäisten tekojen sarjoittamista yhdistämällä sellaisia tietoja, joiden hankkiminen edellyttää telepakkokeinojen käyttämistä.

Rikosoikeutta ja pakkokeinoja on aina pidettävä viimesijaisina keinoina. Näin ollen myös kevyempiä vaihtoehtoja on syytä harkita, esimerkiksi miten voitaisiin saada tietotekninen jälki säilymään pidempään.

Eduskuntakäsittelyssä oleva hallituksen esitys pakkokeinolain muuttamiseksi (HE 222/2010) tulisi poistamaan ainakin osan tutkinnan toimivaltaongelmista, mikäli esitys hyväksytään ehdotetun kaltaisena.

4.5.2.4 Toimivaltuuksista tarkoituksellisen vahingoittamisen rikoksissa

Silloin kun identiteetin väärinkäyttö täyttää jonkin rikostunnusmerkistön kuten kunnianloukkauksen (RL 24:9) tai yksityiselämää loukkaavan tiedon levittäminen (RL 24:8) ja teko toteutetaan verkon julkisella keskustelupalstalla, viranomaisilla on sananvapauslain puitteissa hyvät edellytykset selvittää rikos. Rikos tosin on havaittava ajoissa. Sekä asianomistajan että viranomaisten on oltava nopeita, sillä toimivaltaisen käräjäoikeuden määräys tunnistamistietojen hankkimiseksi (sananvapauslain 17 §) on esitettävä kolmen kuukauden sisällä verkkoviestin julkaisemisesta.

Esitutkintaviranomaisella ei kuitenkaan ole tällä hetkellä toimivaltuutta selvittää samaa tekoa, jos teko toteutetaan tietyn rajatun vastaanottajajoukon piirissä, vaikka tarkemmin valituille vastaanottajille kohdennettu viesti aiheuttaisi asianomistajalle enemmän kärsimystä.

> Esimerkkinä rajatulle vastaanottajajoukolle lähetetystä viestistä voi olla asianomistajaa herjaava viesti, joka on lähetetty sähköpostitse asianomistajan työnantajalle ja kollegoille tai harrastuspiirin suljetulle keskustelupalstalle.

Sananvapauslain pakkokeinot eivät ole käytettävissä rajatulle vastaanottajajoukolle toimitetun viestin lähettäjän selvittämisessä, vaan saman teon esitutkinta edellyttäisi telepakkokeinojen käyttöä, mikä ei ole kunnianloukkausrikoksen tutkinnassa mahdollista. Eduskuntakäsittelyssä oleva hallituksen esitys pakkokeinolaiksi (HE 222/2010) poistaisi tämän ongelman, jos se hyväksytään ehdotetun kaltaisena.

Tutkinta ei aina ole menestyksellistä, vaikka viranomaisten kotimaiset toimivaltuudet olisivatkin ajan tasalla. Verkko on täysin globaali, mutta viranomaisten toimivaltuudet rajoittuvat omaan oikeuspiiriin. Suuri osa sosiaalisen median suosituimmista palveluista sijaitsee Yhdysvaltain verkkoavaruudessa. Osa palveluntarjoajista on rajannut tiedonannon rikoksiin, joista saatava ankarin rangaistus on vähintään 2 vuotta vankeutta tai siten, että kynnys antaa tietoja kunnianloukkauksen kaltaisissa teoissa on erityisen korkea. On vain tunnistettava, että on myös sellaisia tilanteita, joihin ei voi vaikuttaa viranomaisen toimivaltuuksia sääntelevällä kansallisella lainsäädännöllä. Se ei silti ole syy olla korjaamatta kansallisia epäkohtia.

4.5.2.5 Muun identiteettitiedon väärinkäytön torjuntakeinoista

Oikeusministeriö toteaa lausunnossaan (luku 2.6.2): ”Toisen henkilötietojen käyttöön sellaisenaan, ilman taloudellisen hyödyn tarkoitusta tai vahingoittamistarkoitusta, on vain rajoitetusti katsottu olevan tarvetta puuttua rikosoikeudellisin keinoin. Tällainen henkilötietojen käyttäminen voi olla esim. henkilörekisteririkos tai väärän henkilötiedon antaminen.”

Tietoverkoissa tilanne on kuitenkin jossain määrin toinen kuin reaalimaailmassa, sillä tietomassojen automatisoitu yhdistäminen ja tiedon laajempi jakelu mahdollistaa helpommin suuremman vahingon kuin mitä reaalimaailmassa on saatavissa aikaan. Tietoverkossa vahinko voi syntyä, vaikka identiteettitiedon käyttäjällä ei olisi tavoitteena loukata yksittäistä nimettyä kohdetta, eikä tekijä lainkaan ymmärtäisi tekoa tehdessään tekonsa vaikutusta. Esimerkiksi henkilörekisteririkos ei oikeuskäytännön perusteella ilmeisesti täyty, jos tietoja kerätään ilman tarkoitusta loukata rekisteröidyn yksityisyyttä. Väärän henkilötiedon antamista ei puolestaan ole säädetty rangaistavaksi silloin kun kohteena ei ole viranomainen.

Usein esille tuotu uudenkaltainen tekomuoto (ks.3.6.3.3) on yhteisömedioihin kirjautuminen jonkun muun – esimerkiksi julkisuudenhenkilön tai oman opettajan – nimellä ilman vahingoittamistarkoitusta. Kun teko vielä toteutetaan ilman, että kunnianloukkaus (RL 24:8) tai yksityiselämää loukkaava tiedon levittäminen (RL 24:8) täyttyy identiteetin käyttäjän osalta, nimen todellisella haltijalla ei ole mahdollisuutta saada nimenhaltijan nimissä esitettyä sisältöä verkosta pois eikä saada selville kuka teon takana on. Kohdehenkilön yksityisyys kuitenkin kiistatta vaarantuu: Jos nimen todellisen haltijan ystäväpiiri erehtyy pitämään identiteetin käyttäjää nimen todellisena haltijana, identiteetin käyttäjä voi saada tietoonsa nimen haltijan tai tämän lähipiirin yksityisyyden piirin kuuluvaa tietoa. Vaikka asianomistaja kokisi tällä tavoin haittaa, esitutkintaviranomai-

sella ei ole toimivaltuutta käynnistää esitutkintaa tapahtuman selvittämiseksi, kun mikään rikostunnusmerkistö ei täyty. Tällöin ei voida käyttää esimerkiksi sananvapauden käyttämisestä joukkoviestinnässä annetussa laissa tarkoitettua verkkoviestin jakelun keskeyttämistä tai verkkoviestin tunnistamistietojen selvittämistä.

Lainsäätäjä on halunnut taata yhteiskunnassa henkilöille tietyt perusoikeudet. Identiteettivarkaudet voivat loukata oikeutta yksityisyyteen sekä yksityisen viestinnän suojaan. Ne voivat kuitenkin loukata myös omistusoikeutta, silloin kun rikoksella aiheutetaan uhrille taloudellista vahinkoa.

Jotta perusoikeudet voivat konkreettisesti toteutua, lainsäädännön on otettava huomioon ympäristön erityiset ominaispiirteet myös silloin kun ympäristö olennaisesti muuttuu. Samojen vaikutusten tulisi olla kriminalisoituja molemmissa toimintaympäristöissä. Reaalimaailmassa aivan riittävä sääntely ei välttämättä tarjoa vastaavaa suojaa tietoverkossa, sillä tietoverkko eroaa ympäristönä fyysisestä ympäristöstä.

Loukkauksen kohteen suojaamiseen käytettyjen keinojen tulee olla tasapainossa loukkaajaan kohdistuvien rajoitusten kanssa. Henkilön identiteetin suoja voi rajoittaa perustuslain 12 §:ssä säädettyä sananvapautta, koska se estää esiintymisen toisen nimissä. Sananvapaus ei kuitenkaan ole luovuttamaton perusoikeus, jota nytkään saisi käyttää rajoituksetta toisten oikeuksien loukkaamiseen. On vaikea nähdä miksi sananvapauden nimissä tulisi automaattisesti sallia toisen henkilön tiedollisen itsemääräämisoikeuden loukkaaminen ilman erityistä perustetta. Sananvapautta on mahdollista toteuttaa myös syyllistymättä identiteettivarkauteen.

Tiedollinen omistusoikeus eli oikeus omaan nimeen, kuvaan ja hahmoon ja niiden käyttämiseen on yksityisyyteen liittyvä komponentti, jonka tulee koskea kaikkia. Toisen henkilötietojen luvaton käyttö loukkaa henkilön omistusoikeutta omaan identiteettiinsä. Myös sähköisen identiteettitiedon tulisi kuulua itsemääräämisoikeuden piiriin. Henkilöllä tulisi lähtökohtaisesti olla oikeus säilyttää määräysvalta itseään koskevaan informaatioon, pitää se halutessaan salassa tai julkistaa se, ellei laista muuta johdu. Identiteetin luvaton käyttö muiden toimesta ei ole asia, jota oikeusvaltiossa tulisi automaattisesti sallia. Jos henkilön identiteettiä käytetään oikeudettomasti, se rajoittaa hänen tiedollista itsemääräämisoikeuttaan ja rikkoo siten perustuslaissa taattua oikeutta yksityisyyteen. Yksityisyyden menetys voi merkitä uhrille myös taloudellista menetystä tai muuta perinteistä vahinkoa huomattavampaakin haittaa. Siitä voi tulla esimerkiksi merkittäviä sosiaalisia seuraamuksia. Silti tekoa ei tällä hetkellä ole säädetty kaikilta osin rangaistavaksi.

> Ihmisoikeustuomioistuimen ratkaisu K.U. v. Finland, nro 2872/02, EIT 2.12.2008:
> Kysymys yksityiselämän suojan loukkauksesta, kun internetiin alaikäisen nimellä hänen tietämättään seksuaalisluonteisen seuranhakuilmoituksen laittanutta henkilöä ei voitu lainsäädännön puutteista johtuen selvittää eikä saattaa syytteeseen.

Vaikka kriminalisoinnin tulisikin olla viimesijainen keino henkilöiden oikeuksien turvaamiseksi, verkossa ei välttämättä ole muitakaan keinoja. Keskustelujärjestelmiä hallinnoidaan hajautetusti ja globaalisti erilaisissa oikeuskulttuureissa. Ongelma ei siten ole ratkaistavissa keskustelujärjestelmien itsesääntelyn keinoin. Jatkossa tulisikin käynnistää laajempi yhteiskunnallinen keskustelu henkilön tiedollisesta itsemääräämisoikeuden moitittavuudesta.

4.5.3 Uhrin asema identiteettivarkauksissa

Keskeisin epäkohta uhrin asemassa on se, ettei viranomaisilla ole aina toimivaltuutta torjua vahinkoja. Tietoverkossa välttämättömiä toimivaltuuksia, kuten tuomioistuimen päättämää televalvontaa, voidaan käyttää vasta kun tietoverkossa kerättyä identiteettitietoa käytetään väärin. Siinä vaiheessa keräämisestä syntynyt tietotekninen jälki ei kuitenkaan ole enää jäljellä. Huomattavaa taloudellista vahinkoa aiheuttavissa rikoksissa viranomaisella ei ole toimivaltuutta tutkia tekoa ajoissa eikä ehkäistä vahinkoa ennalta, jos teko tapahtuu tietoverkossa, jossa tutkinta edellyttää telepakkokeinojen käyttöä. Eräissä uusissa tekotavoissa taas uhri ei voi saada oikeutta, koska mikään rikostunnusmerkistö ei täyty.

Uhrin oikeusasema ei ole riittävän hyvä myöskään fyysisessä toimintaympäristössä. Vaikka fyysisen maailman identiteettivarkauksien uhrimäärä on verkon identiteettivarkauksia pienempi, niissäkin on syytä kiinnittää huomiota uhrin asemaan. Jos rikollinen on tehnyt uhrin nimissä osoitteenmuutoksen, uhrilla ei ole edes välttämättä tietoa rikoksen tapahtumisesta. Tällöin uhrin luottotiedot vaarantuvat uhrin tietämättä. Lisäksi todistustaakka identiteettivarkauden tapahtumisesta on tällä hetkellä käytännössä rikoksen uhrilla. Vielä senkin jälkeen, kun uhri on tehnyt rikosilmoituksen, uhri joutuu aktiivisesti ja usein toistuvasti vakuuttamaan palveluntarjoajille tai perintäyrityksille, ettei hän ole laskujen aiheuttaja. Lisäksi esimerkiksi ajokortin varastamisen osalta, tekoketjua ei saada välttämättä loppumaan edes tekijän kiinnijäämiseen, ennen kuin itse kortti saadaan tekijältä pois. Ajokorttia kun ei voi mitenkään ”sulkea”, kuten pankki- ja luottokortteja. Passit ja henkilökortit voidaan peruuttaa matkustusoikeuden osalta, mutta niidenkään varastamisen jälkeiseen väärinkäyttöön fyysisessä tunnistamistilanteessa ei auta kuin niiden haltuun saaminen tekijältä.

> HS 2.12.2008. Huijarit nostivat 80 000 euroa pikavippejä väärillä henkilötiedoilla
> Poliisi tutkii laajaa petossarjaa, jossa 13 ihmisen ryhmän epäillään huijanneen itselleen 80 000 euron arvosta pikavippejä. Epäillyt käyttivät hyväkseen 58 ihmisen henkilötietoja. Väärennettyjen ajokorttien avulla he sulkivat ihmisten puhelinliittymiä ja avasivat uusia. Poliisi epäilee ryhmän nostaneen pikavippejä uusien liittymien avulla. Vääriä ajokortteja käyttämällä he myös avasivat pankkitilejä, joihin rahoja ohjattiin. Lisäksi ryhmä teki tilapäisiä osoitteenmuutoksia, joiden avulla he pyrkivät siirtämään rikosten paljastumista. Epäillyt ovat kotoisin Kotkasta, Haminasta ja Lahdesta. Tutkinnassa ei ole saatu täysin selville, miten henkilötiedot ovat joutuneet huijareille. Kotkan ja Kouvolan poliisit tutkivat vuonna 2006 samantyyppistä huijausta. Aiemmassa petossarjassa epäillyt tekijät ovat osin samoja kuin nyt paljastuneessa tapauksessa.
>
> HS 11.8.2010 Henkilö joutui lompakkovarkauden jälkeen petossarjan uhriksi

> Henkilö jäädytti pankki- ja luottokortit välittömästi, mutta tekijä käytti ajokorttia hyväkseen. Tekijä oli ajokorttia näyttämällä ja uhrina esiintyen tehnyt mm. liittymäsopimuksia operaattoreiden kanssa ottaen kylkiäisinä matkapuhelimia ja kannettavia tietokoneita, otti lainoja panttilainaamoista ja lisäksi tekijä oli tarjoavinaan vuokralle muiden omistamia asuntoja uhrin nimissä ottaen takuuvuokran käteisenä. Uhri tekee rikosilmoituksen ja lähetti tiedon siitä operaattoreille ja muille asianosaisille. Tästä huolimatta laskujen ja perintäkirjeiden tulo jatkui pitkään.
>
> HS 3.9.2010. Identiteettivaras sai vankeustuomion. Edellistä esimerkkinä (HS 11.8.2010) koskeva tekijä tuomittiin vuodeksi ja kolmeksi kuukaudeksi ehdottomaan vankeuteen. Tekijä oli tehnyt lukusia rikoksia muiden nimissä. Tekijä syyllistyi kaikkiaan 19 petokseen, 15 väärennykseen, yhteen varkauteen ja yhteen petoksen yritykseen. Tekijä oli esiintynyt kolmen muun naisen nimissä lähes vuoden ajan.

Sittemmin ensimmäisessä esimerkissä käytettyä pikavippejä koskevaa lakia on muutettu. Tältä osin ongelma on poistunut, mutta rikoksessa hyväksikäytetyt haavoittuvuudet, kuten osoitteenmuutokset ja ajokortin käyttö tunnistamisasiakirjana ovat yhä käytettävissä.

Yksityishenkilöt voivat tehdä muuttoilmoituksen ja jakelun keskeytyksen Itellan ja Väestörekisterikeskuksen yhteisessä palvelussa www.muuttoilmoitus.fi. Muuttoilmoituksen voi tehdä internetissä, puhelimitse tai lähimmässä postissa. Sähköinen muutos vaatii tunnistautumisen verkkopankkitunnuksilla, postin käyttäjätunnuksella tai kansalaisvarmenteella. Etenkin soittamalla tehdyt osoitteenmuutokset voivat olla ongelmallisia. Merkittävä enemmistö suomalaisista tekee muuttoilmoituksen väestökirjahallinnolle tai Itellalle nykyisin internetissä. Sähköisen kanavan kautta (internetissä tai puhelimitse) tehtyjen ilmoitusten osuus oli elokuussa 2010 yli 70 % kaikista ilmoituksista. Vuodessa suomalaiset tekevät Itellan ja väestökirjahallinnon osoitteenmuutoksia yhteensä 650 000 kpl.

Identiteettivaras voi fyysisen maailman identiteettivarkauksilla aiheuttaa seurauksia myös sähköiseen asiointiin. Rikoksentekijä voi esimerkiksi väärennetyllä tai varastetulla ajokortilla yrittää hakea uhrin tiedoilla sähköistä varmennetta ja yrittää tehdä uhrin nimissä sitovia oikeustoimia.

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain 12 § mahdollistaa henkilötunnuksen muuttamisen. Väestötietojärjestelmään talletettu henkilötunnus voidaan muuttaa muun muassa, jos muuttaminen on ehdottoman välttämätöntä henkilön suojelemiseksi sellaisissa tilanteissa, joissa hänen terveyteensä tai turvallisuuteensa kohdistuu ilmeinen ja pysyvä uhka tai 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.

Ongelmana on myös, ettei perinteisten petosten ja väärennösten osalta tiedon omistajalle muodostu selkeää rikosoikeudellista asianomistaja-asemaa. Jos erehdytetty henkilö/yritys ei vie asiaa rikostutkintaan, ei sillä, jonka henkilötietoja on käytetty ole mahdollisuutta saattaa asiaa esitutkintaan. Mikäli esimerkiksi velkoja ei vie asiaa tuomiois-

tuinkäsittelyyn, alkuperäisellä vahingonkärsineellä kansalaisella ei ole mahdollisuutta saada oikeutta. Tietoverkossa taas lainsäädäntö pitää henkilöllisyysrikoksen uhrina palveluntarjoajaa, jota on harhautettu toisen henkilötiedoilla, vaikka myös identiteettinsä menettänyt henkilö on tosiasiallinen uhri.

Työryhmässä tarkasteltiin uhrin asemaa myös uudenlaisissa tietoverkoissa ilmenevissä tilanteissa, joissa rikostunnusmerkistö ei tällä hetkellä täyty, vaikka uhri kokee teon loukkaavan perustuslaissa taattuja oikeuksiaan (PL 2. luvun 10 §). Työryhmässä katsottiin, että esimerkiksi esiintyminen ja oman mielipiteensä ilmaiseminen toisen henkilön nimissä loukkaa toisen henkilön oikeuksia, vaikkei mielipiteenilmaisusta aiheutuisikaan aineellista vahinkoa. Aikaisemmin tällaisen teon kriminalisointiin ei ole nähty lainkaan tarvetta. Tietoverkko on kuitenkin saattanut jossain määrin muuttaa tilannetta. ”Virheellinen” mielipide on nyt näkyvillä käytännöllisesti katsoen ikuisesti, se on tavoitettavissa paljon laajemmin kuin reaalimaailmassa ja sen korjaaminen voi olla mahdotonta.

4.6 Biometria

Sisäasiainministeriön poliisiosasto ja Poliisihallitus katsovat, että biometrian hyödyntäminen mahdollistaa automaation ja oikein toteutettuna luotettavamman tunnistamisen. Automaation avulla prosessit saadaan nopeammiksi ja halvemmiksi.

4.6.1 Biometriset tunnisteet viranomaisasiakirjoissa

Rikollisjärjestöt keräävät oikeilta omistajilta varastettuja tai kadonneita tunnistusasiakirjoja järjestelmällisesti kokoelmiksi, joista rikolliset voivat hankkia itselleen sopivan. Mitä suurempi kokoelma on, sitä todennäköisemmin asiakkaalle löytyy joukosta asiakirja, jossa oleva kuva on silmämääräisesti arvioiden riittävän samannäköinen.

Väärinkäyttäjät suosivat siruttomia asiakirjoja, sillä silmämääräisesti riittävän samannäköinen kuva ei riitä huijaamaan henkilöllisyyden todentamiseen käytettävää koneellista kasvontunnistusta. Tällä hetkellä jo yli 70 maata maailmassa myöntää passeja, joissa on sirulle tallennettu valokuva koneellista kasvontunnistusta varten, ja määrä lisääntyy jatkuvasti. EU-maissa on astuttu jo seuraava askel ottamalla passeissa käyttöön myös sormenjäljet. Biometrisen tunnistuksen avulla voidaan tehokkaasti estää väärinkäyttäjiä hyödyntämästä kadonneita ja varastettuja tunnistusasiakirjoja.

Biometristen tunnisteiden tallentaminen henkilöllisyyttä osoittaviin asiakirjoihin on erittäin hyvä keino estää ja vähentää identiteettivarkauksia. Passinhakija antaa tällä hetkellä biometrisiksi tunnisteikseen kasvokuvansa ja kaksi sormenjälkeä, ja turvalliselle passisirulle tallennettuina ne mahdollistavat vahvan tunnistamisen. Haasteena tällä hetkellä on passintarkastusjärjestelmien saattaminen ajantasaisiksi siten, että biometrinen tunnistaminen tapahtuu luotettavasti ja nopeasti.

Biometrisia tunnisteita ollaan lisäämässä useille asiakirjoille. EU:n oleskelulupa-asetuksen (EY) N:o 1030/2002 muuttamista koskevan neuvoston asetuksen (EY) N:o 380/2008 mukaisesti EU-maissa on otettava tarramuotoisten oleskelulupien sijaan biometriset tunnisteet sisältävät oleskelulupakortit käyttöön viimeistään toukokuussa 2011 (sormenjälkien osalta toukokuussa 2012). Eduskunnalle on 16.7.2010 annettu hallituksen esitys (HE 104/2010 vp) koskien biometristen tunnisteiden käyttöönottoa oleskeluluvissa. Kolmansien maiden kansalaisille myönnettävä oleskelulupakortti sisältäisi sirun, joka olisi samanlainen kuin passisirukin ja tulisi siten sisältämään sekä kasvokuvan että kaksi sormenjälkeä.

Myös EU-kansalaisen kolmannesta maasta tulevalle perheenjäsenelle myönnettävään oleskelukorttiin (ei oleskelulupa) on edellä mainitussa hallituksen esityksessä ehdotettu lisättäväksi biometriset tunnisteet. Tätä neuvoston oleskelulupa-asetus ei kuitenkaan edellytä.

Sisäasiainministeriön poliisiosasto ja Poliisihallitus ehdottavat lisättäväksi biometrisia tunnisteita lisättäväksi myös henkilökorteille samoin perustein kuin passilain osalta. Biometristen tunnisteiden käyttöönotto edellyttää henkilökorttilain muutosta. Lisäksi myös viisumeita varten ryhdytään ottamaan sormenjälkiä. Tästä tarkemmin osiossa 4.6.1.1.

Tulevaisuuden biometrisiä tunnisteita julkishallinnossa saattavat olla sormenjäljen lisäksi iiris ja sormen verisuonikuviot. Verisuonikuviolla on tulevaisuuden tunnisteratkaisuna moneen käyttötarkoitukseen sopivia piirteitä: vaikea kopioida toiselta, vaikea väärentää, tunnistusta on vaikea tehdä salaa eikä tunnistus välttämättä vaadi edes kosketusta mihinkään laitteeseen.

Sirut ja biometriset tunnisteet ovat tulleet matkustusasiakirjoihin vasta vähän aikaa sitten, ja vie vielä aikaa, ennen kuin niistä tulee täysin arkipäiväinen osa henkilön tunnistusta.

Uhkakuvat biometristen tunnisteiden väärinkäyttömahdollisuuksien vaaroista eivät niinkään liity viranomaistoimintaan vaan hallitsemattomaan yksityisten toimijoiden käyttöön. Biometrian käyttö yksityisellä puolella tulee yleistymään.

4.6.1.1 EU:n yhteinen viisumitietojärjestelmä

Viisumeiden osalta EU:n jäsenmaiden yhteinen viisumitietojärjestelmä VIS (Visa Information System) on merkittävä uudistus, jossa jokaisen maan kansallisesta viisumitietojärjestelmästä tullaan siirtämään yhteiseen tietokantaan Schengen-viisumihakemustietoja ja hakijan biometriset tunnisteet (kasvokuva ja sormenjäljet). Jäsenmaiden konsulaatit ja muut toimivaltaiset viranomaiset voivat tallentaa tietokantaan viisumihakemustietoja sekä hakea tietoa viisuminhakemuksista ja niihin tehdyistä päätöksistä.

VIS:stä on tulossa maailman suurin tietojärjestelmä, joka tulee sisältämään tietoa 80–100 miljoonasta viisuminhakijasta. Kaikkiaan 29 Schengen-maata tulee liittymään järjestelmän käyttäjiksi. VIS:n tulevat ottamaan käyttöön Alankomaat, Belgia, Espanja, Italia, Islanti, Itävalta, Kreikka, Latvia, Liettua, Luxemburg, Malta, Norja, Puola, Portugali, Ranska, Ruotsi, Saksa, Slovakia, Slovenia, Suomi, Sveitsi, Tanska, Tsekki, Unkari ja Viro. Myöhemmin järjestelmän käyttäjiksi liittyvät myös Bulgaria, Kypros, Liechtenstein ja Romania.

VIS:n tarkoitus on parantaa yhteisen viisumipoliitiikan täytäntöönpanoa, konsuliyhteistyötä ja keskusviisumiviranomaisten välistä yhteydenpitoa. Yhteinen viisumitietojärjestelmä helpottaa Schengen-viisumihakemuksia ja niihin liittyvää päätöksentekoa koskevaa tietojenvaihtoa jäsenvaltioiden välillä. Viisumihakemusmenettelyjen keventäminen tulee olemaan mahdollista yhteisessä viisumitietokannassa olevien tietojen avulla, esim. viisuminhakuhistoria pystytään helposti toteamaan. Järjestelmän avulla pystytään ehkäisemään mahdollisimman edullisen viisumikohtelun etsimistä (visa shopping).

Yhteinen viisumitietojärjestelmä edistää viisumeihin ja henkilöllisyyksiin liittyvien väärinkäytösten torjuntaa ja helpottaa niiden toteamista. VIS helpottaa tarkastuksia Schengenin ulkorajojen ylityspaikoilla ja jäsenvaltioiden alueella. Järjestelmän avulla Schengenin alueelle pyrkiviä ja siellä oleskelevia kolmansien maiden viisumivelvollisia kansalaisia voidaan paremmin tunnistaa. Tämä tukee myös menettelyjä turvapaikkahakemuksia käsiteltäessä ja laittomien siirtolaisten palauttamisessa lähtömaahan. VIS auttaa jäsenvaltion sisäiseen turvallisuuteen kohdistuvien uhkien ehkäisyä. Viranomaiset voivat käyttää järjestelmän tietoja terroristiuhkien ja muiden vakavien rikosten ehkäisyyn, havaitsemiseen ja tutkintaan.

VIS-järjestelmä ja sen käyttö perustuvat Euroopan parlamentin ja neuvoston asetukseen 767/2008 viisumitietojärjestelmästä (VIS) ja jäsenmaiden välisestä tietojenvaihdosta koskien lyhytaikaisia viisumeita (VIS-asetus), neuvoston päätökseen 2008/633/JHA jäsenvaltioiden nimeämien viranomaisten ja Europolin pääsystä tekemään hakuja viisumitietojärjestelmästä (VIS) terrorismirikosten ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi (VIS-päätös), neuvoston päätökseen VIS:n perustamisesta (2004/512/EY), Schengenin rajasäännöstön muutosasetukseen 81/2009 ja Euroopan parlamentin ja neuvoston asetukseen (EY) N:0 810/2009 (viisumisäännöstöön).

Alkuperäisen suunnitelman mukaan VIS:n piti tulla käyttöön maaliskuussa 2007. Käyttöönoton mahdollistava neuvoston päätös jäsenvaltioiden nimeämien viranomaisten ja Europolin pääsystä tekemään hakuja viisumitietojärjestelmästä (VIS) terrorismirikosten ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi, tehtiin kuitenkin vasta syksyllä 2008, jonka jälkeen sovitun aikataulun mukaan VIS olisi tullut ottaa käyttöön 29.5.2009. Jäsenmaiden keskusjärjestelmään vaatimien muutostarpeiden vuoksi VIS:n käyttöönottoa siirrettiin alkavaksi 21.12.2009, josta se siirtyi edelleen vuodella eteenpäin. Sittemmin EU-komissio on ilmoittanut keskusjärjestelmän testaus-

ja suoritusarvo-ongelmista, ja keskusjärjestelmän olevan valmis tuotantoon kesäkuussa 2011. Käyttöönottoaikataulu riippuu jäsenmaiden kansallisesta valmiudesta sekä konsulaattien että rajanylityspisteiden osalta.

Käytännössä uudistus tarkoittaa, että viisuminhakijoilta otetaan edustustoissa sormenjäljet (10 sormea) ja ulkorajatarkastukset aloitetaan viisuminumerolla tai viisuminumerolla ja sormenjäljillä. Sormenjälkitarkastusten käyttöönoton osalta jäsenmaat voivat soveltaa kolmen vuoden siirtymäaikaa. Poliisilaitoksissa VIS tulee käyttöön poliisin VIS-asetuksessa mainittujen oikeuksien (mm. henkilöiden todentaminen, henkilöiden tunnistaminen, ulkomaalaisvalvonta) osalta EU:ssa määritellyn VIS:n käyttöönottoaikataulun mukaisesti. VIS:n käyttäjäorganisaatioita ovat edustustojen lisäksi rajavartiolaitos, paikallispoliisi, suojelupoliisi, keskusrikospoliisi, Maahanmuuttovirasto ja tulli. Poliisi ei enää uuden viisumisäännöstöä koskevan kansallisen tulkinnan mukaisesti myönnä viisumeita, vaan jatkaa, mitätöi tai kumoaa viisumin.

4.6.2 Biometrisen tunnistuksen luotettavuus

Näytteenottotilanteen olosuhteet vaikuttavat ratkaisevasti biometrisen tunnistuksen luotettavuuteen. Biometrisen tunnisteen alkuperäisessä rekisteröinnissä tapahtuneet virheet vaikuttavat kaikkiin tuleviin tunnistustapahtumiin, ja vastaavasti yksittäisessä tunnistustilanteessa virheellisesti otetut biometriset näytteet voivat mitätöidä tunnistuksen luotettavuuden.

Biometrisen tunnisteen luotettavuus riippuu myös vertailupopulaatiosta; jos henkilö x on tunnistettava erilleen muista työntekijöistä samassa työyhteisössä, esimerkiksi kulunvalvonnassa, riittää luultavasti kasvontunnistus ja varmuudella sormenjäljet; mutta jos vertailupopulaatio on miljoonaluokkaa, koneellinen kasvontunnistus alkaa olla epäluotettavaa eikä sormenjälkitunnistuskaan enää ole aukotonta. DNA-vertailussa varmuus on nykyteknologialla 1 000 000 000:1 (teoriassa suhde on jyrkempi, mutta nykymenetelmiin sisältyy virhemahdollisuuksia), eli miljardin henkilön joukosta löytyy yksi henkilö, josta saadaan identtinen näyte henkilö x:n kanssa. Jos aineistoa on mielivaltaisen paljon, erottelu voidaan tehdä, mutta näin ei tyypillisesti ole.

Koon lisäksi myös populaation laatu voi vaikuttaa tunnistusvarmuuteen. Jos miespuolisella henkilöllä on identtinen kaksosveli, koneellinen kasvontunnistus ei luultavasti kykene erottamaan heitä toisistaan, minkä lisäksi heidän DNA:nsa on identtinen. Laboratoriossa tapahtuva manuaalinen kasvovertailu tuottaa teoriassa ennen pitkää oikean vastauksen, jos käytettävissä on mielivaltaisen paljon vertailuaineistoa, mutta tämä on käytännössä harvoin tilanne. Sormenjäljet ovat identtisilläkin kaksosilla erilaiset.

4.6.3 Biometrisen tunnistamismenetelmän valinta

Oli kyse sitten yksityisestä tai julkisesta sektorista, biometrisen tunnistamistavan valintaa säätelevät seuraavat tekijät:

1. Yleisyys: Jokaisella tai lähes jokaisella järjestelmän käyttäjällä on kyseinen tunniste. Kaikilla ihmisillä ei ole sormia, joista voitaisiin ottaa sormenjäljet, tai silmiä, joiden iiriksiä voitaisiin käyttää tunnistukseen, mutta toisaalta kaikilla on DNA.

2. Yksilöllisyys: Tunnisteen on eroteltava kaikki järjestelmän käyttäjät toisistaan. Esimerkiksi identtisillä kaksosilla on erilaiset sormenjäljet mutta sama DNA.

3. Pysyvyys: Tunniste ei saa muuttua liikaa ajan kuluessa. Nykytietämyksen mukaan sormenjäljet pysyvät tunnistuskelpoisina hyvin pitkään, kun taas kasvot saattavat muuttua ajan myötä paljonkin. DNA pysyy käytännössä muuttumattomana koko elämän ajan.

4. Kerättävyys: Tarvittava biometrinen näyte kyetään ottamaan vaivattomasti, nopeasti ja mahdollisimman pienin teknisin järjestelyin. Esimerkiksi sormenjälkien ottaminen ja vertailu on nykytekniikalla nopeaa ja yksinkertaista, ja epäonnistumisprosentti on pieni. DNA-näytteen ottaminen vie enemmän aikaa, ja varsinainen vertailu vie huomattavan kauan. Kerättävyyteen liittyy myös se, kuinka kalliita ja vaikeasti saatavia tunnistuksessa tarvittavat laitteet ovat.

5. Hyväksyttävyys: Ihmisten on voitava hyväksyä tunnistustapa. Osa tunnistustavoista, kuten DNA, herättää pelkoja väärinkäyttövaaroista. Vastaavasti osa ihmisistä vastustaa sormenjälkitunnistusta, koska yhdistää sen rikostutkintaan. Kasvontunnistus puolestaan on useimmille helpoimmin hyväksyttäviä tunnistusmuotoja, koska ihmiset tunnistavat arkielämässään toiset ihmiset useimmiten kasvoista, mutta tähän liittyy kulttuurikohtaisia eroja

6. Toimivuus: Menetelmän on oikein käytettynä kyettävä paljastamaan suurella todennäköisyydellä, onko tunnistettava henkilö se joka väittää olevansa.

7. Huijattavuus: Järjestelmän huijaaminen väärennetyillä tai toiselle henkilölle kuuluvilla tunnisteilla on oltava mahdollisimman vaikeaa. Huijausmahdollisuudet jakautuvat kolmeen osaan:

    - Kuinka helposti järjestelmä erehtyy luulemaan annettua näytettyä samaksi kuin jokin toinen näyte, vaikka ne olisivat tosiasiassa erilaisia (tunnistustarkkuus)? Esimerkiksi kasvontunnistuksessa tällaiset virheet ovat mahdollisia, kun taas sormenjälkitunnistuksessa ne ovat harvinaisia, mikäli näytteet ovat hyvälaatuisia.

    - Kuinka helposti toisen henkilön biometriset tunnisteet ovat hankittavissa väärinkäyttöä varten? Kasvokuva on yleensä erittäin helppo saada, ja sormenjäljet ovat poimittavissa esineistä, joita kohdehenkilö on käsitel-

lyt. DNA:n voi kerätä irronneista hiuksista tai syljestä. Sormenpään tai kämmenen verisuonikuviot ovat esimerkki tunnisteesta, jota on vaikea kerätä ilman erityislaitteita ja -osaamista.

- Kuinka helppoa on syöttää järjestelmälle väärennetty tunniste? Tämä riippuu ensisijaisesti siitä, tapahtuuko näytteenotto valvotusti. Jos tapahtuu, sormenpäihin liimatut keinojäljet ja kasvoihin tehty voimakas maskeeraus todennäköisesti paljastuvat. Jos näytteenotto tapahtuu kotioloissa kenenkään näkemättä, väärinkäyttäjä voi simuloida aitoa tilannetta kuinka mutkikkailla teknisillä järjestelyillä tahansa.

Jokaisella biometrisellä tunnistustavalla on erilaiset ominaisuudet edellä esitettyihin vaatimuksiin nähden. Biometrisen tunnistamisen käyttötarkoitus, käyttötavat ja käyttöympäristö vaikuttavat voimakkaasti eri vaatimusten painotuksiin.

4.6.4 Biometrinen tunnistaminen yksityisellä sektorilla

On mahdollista, että yksityinen sektori tarvitsee tulevaisuudessa henkilöllisyyden biometrista todentamista, ja keskusteltavaksi voi tulla se, onko yksityisellä sektorilla mahdollisuutta hyödyntää valtion takaamien tunnistusasiakirjojen sisältämiä biometrisia tunnisteita. EU-lainsäädännössä on tarkasti rajattu, mihin passien biotunnisteita saa käyttää, joten yksityisen sektorin hyödynnettäviksi tarkoitetut biotunnisteet olisi tallennettava jollekin muulle alustalle.

4.6.4.1 Biometristen tunnisteiden säilytys

Jotta henkilön tunnistaminen biometrisesti olisi ylipäätään mahdollista, jossain on säilytettävä biometristä näytettä, kuten esimerkiksi sormenjälkeä, johon henkilöltä tunnistustilanteessa otettavaa näytettä verrataan. Vertailunäytettä voidaan säilyttää joko keskitetyssä rekisterissä, tunnistettavan henkilön hallussa olevan tunnistusvälineen muistissa tai molemmissa.

Kun puheena on valtion takaama tunnistustapa, keskitetyn rekisterin on oltava viranomaisen hallinnassa ja vastaavasti biotunnisteen sisältävän tietovälineen on oltava viranomaisen myöntämä.

Jos tunnisteita säilytetään rekisterissä, vertailunäyte on otettava tunnistuspaikassa ja sitä on tavalla tai toisella verrattava rekisterissä olevaan tunnisteeseen. Tämä edellyttää, että tunnistajalla on hallussaan tunnisteiden keräämiseen tarvittava laite. Tunnistaja voi omistaa laitteen tai se voi teoriassa olla myös valtiolta vuokrattu sinetöity laite. Käytännössä sinetöityjen laitteiden hallinnointi olisi valtiolle hyvin kuormittavaa jo tarvittavien laitevolyymien takia.

Jos yksityiseen sektoriin kuuluva tunnistaja omistaa biotunnisteiden keräämiseen tarkoitetun laitteen, on aina olemassa vaara, että sen kautta kulkeneista tunnisteista jää kopio tunnistajan tietojärjestelmiin. Tällöinkin muodostuu viranomaisvalvonnan ulkopuolelle jäävä tunnisterekisteri. Valtion takaaman biometriikkaratkaisun tulisi tähdätä siihen, ettei tunnistajalla olisi mahdollisuutta kerätä sen avulla omaa rekisteriä tunnistettavien henkilöiden biotunnisteista.

4.6.4.2 Biometrisen näytteen ottaminen

Kuten edellä on todettu, biometrisen tunnistamisen luotettavuus riippuu siitä, kuinka valvotuissa oloissa biometrinen näyte otetaan. Valtion takaamassa tunnistusmenetelmässä on lähdettävä siitä, että alkuperäinen näyte on joka tapauksessa otettu valvotusti ja tallennettu turvallisesti rekisteriin tai tunnistusvälineen muistiin, joten hankaluudet liittyvät nimenomaan myöhemmissä tunnistustilanteissa tapahtuvaan näytteenottoon.

Näytteenoton valvonta on haasteellista aina, kun toimitaan yksityisellä sektorilla, koska tunnistusolosuhteet vaihtelevat paljon ja henkilökunta saattaa vaihtua nopeassa tahdissa. Lisäksi yksityisellä sektorilla ei ole käytössään pääsyä samoihin rekistereihin, joita hyödyntämällä julkisella puolella voidaan tunnistaminen tehdä luotettavasti ilman luotettavaa henkilöllisyyttä osoittavaa asiakirjaakin. Erityisen suuria vaikeuksia kohdataan verkossa tapahtuvassa tunnistautumisessa. Jos henkilö asioi verkossa kotoaan käsin, näytteenottoa on lähes mahdotonta valvoa.

5 Johtopäätökset ja toimenpidesuositukset

5.1 Henkilöllisyyden luominen

Henkilöllisyys syntyy, kun henkilön tiedot viedään väestötietojärjestelmään, joka nauttii julkista luotettavuutta. Suomessa on kattava väestötietojärjestelmä ja täten kansalaisilla on valtion takaama henkilöllisyys. Henkilö voi käyttää tätä henkilöllisyyttä sekä fyysisessä että sähköisessä toimintaympäristössä. Valtion viranomainen myöntää henkilöllisyyttä osoittavat asiakirjat ja joko viranomainen tai yksityinen taho vastaavasti sähköisessä asioinnissa käytetyt henkilöllisyyttä osoittavat varmenteet. Varmenteidenkin osalta tunnistaminen perustuu viranomaisten myöntämiin asiakirjoihin. Luotettavan henkilöllisyyden taustalla onkin kyse viranomaistoiminnan toteuttamisesta ja kansalaisten perustuslaillisten oikeuksien toteutumisesta ja turvaamisesta.

Työryhmä toivoo, että tässä raportissa esitetty jäsentynyt näkemys termeistä ja henkilöllisyydestä saataisiin vietyä laajalti eri foorumeille, joissa asioista puhutaan. Raportin alussa esitettyjen määritelmien ja niille annettujen merkitysten toivotaan ainakin ja ensi vaiheessa kansallisella tasolla yleistyvän. Työryhmään osallistuneiden tahojen tulisi omassa työssään edistää määritelmien tunnettuutta sellaisina kuin ne tässä raportissa esitetään. Työryhmä ei kuitenkaan esitä varsinaisia toimenpidesuosituksia aiheesta.

Lisäksi sisäasiainministeriö ja Poliisihallitus katsovat, että myös jatkossa poliisilla tulisi olla muiden toimijoiden ohella rooli sähköisessä toimintaympäristössä viranomaisen varmenteita myönnettäessä, erityisesti tunnistamisen osalta.

5.2 Henkilöllisyyden suojaaminen

Työryhmä toteaa, että perustuslain 124 § hallintotehtävän antamisesta muulle kuin viranomaiselle suojaa henkilöllisyyttä yhdessä yksityiselämän suojaa sääntelevän perustuslain 10 §:n kanssa. Valtion tuleekin suojata henkilöllisyyttä samantasoisesti sekä fyysisessä että sähköisessä toimintaympäristössä turvallisten tunnistamisprosessien sekä lainsäädännön keinoin.

5.3 Toimivaltaiset viranomaiset

Työryhmä toteaa, että viranomaiset pyrkivät entistä tiiviimpään yhteistyöhön toistensa kanssa ja pyrkivät kansalaisten kannalta tarkoituksenmukaisiin ratkaisuihin.

5.4 Ulkomaalaisen varmistamaton henkilöllisyys

Työryhmä katsoo, että ulkomaalaisten varmistamattoman henkilöllisyyden osalta tulisi määritellä eri lainsäädännöissä käytetyt termit ja pitää huolta siitä, että niitä käytetään vain oikeassa kontekstissa. Pääsääntöisesti tulee käyttää termiä ”henkilöllisyyttä ei ole voitu varmistaa”, kun ulkomaalainen ei ole pystynyt esittämään luotettavaa asiakirjaselvitystä henkilöllisyydestään.

5.5 Tunnistaminen ja tunnistamisasiakirjat

Työryhmä toteaa, että ajokortin käyttöön tunnistamisasiakirjana liittyy riskitekijöitä, jotka ovat tulleet myös tehdyssä riskianalyysissä esille. Työryhmä katsoo, että ajokortin asemaa tunnistamisasiakirjana tulisi tarkastella uudelleen ja osoitteenmuutoksen tekemisen tulisi olla mahdollista vain vahvasti tunnistetulle asiakkaalle.

Työryhmä toteaa, että tältä osin palveluntarjoajiin voidaan vaikuttaa muun muassa ohjeistuksia muuttamalla, ja kansalaisten toimintaan voidaan vaikuttaa tietoisuutta lisäämällä. Lisäksi lakia vahvasta sähköisestä tunnistamisesta ja sähköisestä allekirjoituksesta on syytä muuttaa siinä vaiheessa, jos tunnistamisasiakirjaksi yleisesti kelpuutetaan ainoastaan passi tai henkilökortti. Lyhyemmällä tähtäimellä poliisi voisi resurssiensa puitteissa auttaa vahvistamaan yksityisten palveluntarjoajien ensitunnistamisprosesseja ja osallistua kouluttamiseen.

Työryhmä ehdottaa ajokorttien, henkilökorttien ja passien sulkulistapalvelun toteuttamismahdollisuuden selvittämistä lainsäädännön, kustannusten ja teknologian osalta.

Työryhmä ehdottaa passin ja henkilökortin yhteismyöntöprosessin mahdollisuuden selvittämistä. Etuna olisi henkilökortin mahdollinen hinnan aleneminen ja edullisempi henkilökortti olisi myös vaihtoehto ajokortille tunnistamisasiakirjana.

Työryhmä toteaa myös, että Kela-kortin käyttöä tunnistamiseen olisi syytä välttää.

Sekä asiakirjoja että henkilöitä koskevan tunnistamisen merkitystä tulee entisestään korostaa. Työryhmä katsoo, että tunnistamiseen liittyvä koulutus on erittäin tärkeää kaikkien toimijoiden osalta. Fyysisen tunnistamisen turvallisuus on tällä hetkellä kiinni pitkälti tunnistamistehtävissä toimivien henkilöiden tarkkuudesta ja ammattitaidosta sekä käytettävistä apuvälineistä. Lisäksi tunnistamisasiakirjoja on niin paljon, ettei niitä ole kaikkia mahdollista hallita. Lyhyellä tähtäimellä tulisi kiinnittää huomiota tunnistustehtävissä toimivien henkilöstöryhmien kouluttamiseen ja motivointiin. Tunnistamiseen ja tunnistamisasiakirjoihin liittyvää koulutusta tulee tehostaa ja selvittää mahdollisuutta, että viranomaisten lisäksi myös yksityiselle sektorille voitaisiin tarjota tunnistamiskou-

lutusta. Tunnistamista tekevien on oltava riittävästi koulutettuja ja heillä tulisi olla käytössä riittävät tekniset apuvälineet.

Työryhmä katsoo, että yhteistyötä tulee parantaa yksityisen puolen ja viranomaisten välillä. Viranomaiset voisivat resurssiensa puitteissa esimerkiksi kouluttaa yksityisen sektorin omia tunnistuskouluttajia sekä tarjota verkkopohjaisia oppimistyökaluja.

Työryhmä pitää tärkeänä tiedotuskampanjaa eri asiakirjojen turvallisuudesta sekä kansalaisille, viranomaisille että yksityiselle sektorille.

Lainsäädäntöön liittyvät työryhmässä esiin tulleet ehdotukset:

- Työryhmä ehdottaa turvapaikanhakijan asiointikortin myöntämisen selvittämistä turvapaikanhakijoiden alkuvaiheen asiointia varten. Työryhmä ehdottaa selvityshankkeen asettamista tarkempien käytännön jatkotoimien ja lainsäädäntömuutostarpeiden selvittämiseksi. Työryhmän työhön osallistuisivat ainakin edustajat Poliisihallituksesta, sisäasiainministeriön maahanmuutto-osastolta ja poliisiosastolta, ulkoasiainministeriöstä ja Maahanmuuttovirastosta sekä Finanssialan keskusliitosta ja Finanssivalvonnasta. Esiselvitys laadittaisiin arviomuistion muotoon, jossa selvitettäisiin muun muassa asiointikortin oikeusvaikutukset tunnistamisasiakirjana ja muutoin, saajatahot, määrät, vaikutukset poliisin toimintaan jne.

- Sisäasiainministeriön poliisiosasto ja Poliisihallitus ehdottavat henkilökorttilain muutosta, jossa kortteihin lisättäisiin biometriset tunnisteet, kuten passeissa ja oleskelulupakorteissa.

- Sisäasiainministeriön poliisiosasto ja Poliisihallitus esittävät henkilöllisyyttä osoittavia asiakirjoja koskevan lainsäädännön tarpeellisuuden selvittämistä. Sisäasiainministeriö ja Poliisihallitus ehdottavat selvityshankkeen asettamista aiheesta siten, että selvitys laadittaisiin arviomuistion muotoon. Lainsäädännössä tulisi määritellä turvalliset henkilöllisyyden osoittavat asiakirjat sekä Suomen kansalaisille että ulkomaalaisille. Lain tasoisesti tulisi määritellä henkilöllisyyttä osoittavat asiakirjat Suomen kansalaisten ja ulkomaalaisten osalta. Myös turvallisen fyysisen tunnistamisen vähimmäismenettelyt tulisi määritellä laissa. Vahvasta sähköisestä tunnistamisesta säädetään jo erikseen omalla laillaan.

5.6 Kansalaisvarmenne ja tulevaisuuden käyttömuodot

Valtiovarainministeriön vetämä valtion varmennepalvelujen uudelleen organisointia selvittävä työryhmä on päättänyt työnsä. Ratkaisu kansalaisvarmenteen tulevaisuudesta on ilmoitettu tehtäväksi vuoden 2011 aikana. Jatkotyön tarkempi organisointi ei ole vielä tiedossa.

5.7 Identiteettivarkaudet

Identiteettivarkauksissa identiteettitietoa kerätään ja käytetään siten että teolla

- tavoitellaan suurta taloudellista rikoshyötyä tai
- tavoitellaan identiteetin todellisen haltijan oikeuksien loukkaamista tai
- loukataan identiteetin todellisen haltijan perustuslaissa säädettyjä oikeuksia, mutta ilman varsinaista hyödyn hankkimisen tai kohteen vahingoittaminen tavoitetta

Työryhmässä identiteettivarkauksia tarkasteltiin erikseen reaalimaailmassa ja tietoverkossa, sillä tietoverkko muuttaa varsin olennaisesti identiteettitietoon kohdistuvaa uhkaa. Fyysisessä maailmassa identiteettitiedon loukkaukset ovat yksittäistapauksia, jolloin niistä aiheutuva vahinko on hallittavissa – erityisesti kun rikostorjunnan toimivaltuudet ovat reaalimaailmassa riittävät. Sen sijaan tietoverkossa identiteettivarkauksilla hankittu rikoshyöty voi olla valtava ja seuraukset yksittäisen rikosuhrin kannalta huomattavat, mutta esitutkintaviranomaisilla ei silti ole aina toimivaltuutta selvittää tapauksen tosiasioita.

5.7.1 Perusoikeusvaikutukset

Työryhmä katsoo, ettei perustuslain 10 §:n yksityisyyden suoja ja siitä johdettava tiedollinen itsemääräämisoikeus ja tiedollinen omistusoikeus eivät aina toteudu, koska kansalaisella ei ole todellisuudessa mahdollisuutta hallita omaa henkilöllisyyttään uusissa toimintaympäristöissä.

Hyöty- tai vahingoittamistarkoituksessa toteutettujen tekokokonaisuuksien lisäksi työryhmä tarkasteli myös muunlaisia uudenlaisia identiteettiloukkauksia, joissa mikään rikostunnusmerkistö ei täyty, vaikka teon kohde kokee oikeuksiaan loukatun. Henkilön nimissä esiintyminen rajoittaa henkilön tiedollista itsemääräämisoikeutta ja rikkoo siten perustuslaissa taattua oikeutta yksityisyyteen ja kunnian loukkaamattomuuteen. Työryhmä katsoo, että jatkossa tulisi käydä laajempi yhteiskunnallinen keskustelu siitä onko henkilön nimissä esiintyminen ilman henkilötietojen haltijan lupaa asia, joka tulisi jatkossakin sallia vai tulisiko henkilöllä olla oikeus tiedolliseen itsemääräämisoikeuteen. Tietoverkko on muuttanut tilannetta olennaisesti, sillä tietoverkossa virheellinen tieto leviää laajalle ja säilyy kauan.

Perustuslaillinen suoja voi olla myös vaarassa, koska poliisi ei voi aina tosiasiallisesti tutkia tiettyjä väärinkäytöksiä, jos ne tapahtuvat tietoverkoissa. Asia on keskeinen niin henkilön itsensä, sisäisen turvallisuuden sekä tietoyhteiskunnan toiminnan kannalta. Työryhmä katsoo, että perustuslain 10 §:stä voidaan johtaa, että kansalaisella tulisi olla käytössä tieto, keinot ja tuki identiteettivarkauksien suojautumiseen ja jälkihoitoon. Yh-

teiskunnan tulisikin taata nykyistä parempi suoja identiteettitietoon liittyvien loukkausten kohteelle, sekä reaalimaailmassa että tietoverkossa.

5.7.2 Uhrin aseman turvaaminen identiteettivarkauden jälkeen

Työryhmä katsoo, että identiteettivarkauden uhrilla tulisi olla nykyistä paremmat edellytykset toipua identiteettitiedon kaappaamisesta ja taloudellisesta väärinkäytöstä ilman kohtuutonta vaivannäköä. Lisäksi uhrilla ei ole aina välttämättä rikosprosessissa asianosaisasemaa. Ensimmäisenä toimenpiteenä työryhmä ehdottaa toimintaohjeen tekemistä henkilöllisyysvarkauden uhrin jatkotoimista. Pidemmällä tähtäimellä tulisi tarkastella mahdollisuutta rakentaa keskitetty ilmoitusjärjestelmä, jonka kautta tieto identiteettikaappauksista voisi välittyä nopeasti velkojille ja viranomaistahoille. Työryhmä ehdottaakin selvitystä, onko keskitetyn ilmoitusjärjestelmän luominen käytännössä mahdollista.

5.7.3 Rikos- ja prosessioikeuden keinot uhrin aseman turvaamiseksi

Identiteettitiedon käyttäminen väärin joko hyödyn hankkimiseksi tai kohteen vahingoittamiseksi on yleensä kriminalisoitu. Työryhmä katsoo, että lainsäädäntö tarjoaa tältä osin riittävän suojan rikoksen uhreille.

Vaikka tiedon käyttäminen rikoshyödyn hankkimiseksi onkin kriminalisoitu, tietoverkossa se ei kuitenkaan riitä rikoksen saattamiseksi oikeusprosessiin, sillä siinä vaiheessa kun kerätyn identiteettitiedon oikeudeton käyttäminen alkaa, alkuperäistä epäillyn jäljille johtavaa identiteettitiedon keräämisestä syntynyttä tietoteknistä jälkeä ei yleensä ole enää olemassa. Tekotavasta riippuen tiedon keräämistä joko ei ole kriminalisoitu lainkaan tai se on kriminalisoitu tavalla, joka ei lainkaan mahdollista menestyksellistä esitutkintaa tietoverkossa.

Työryhmä katsoo, että jatkokäsittelyssä tulisi tarkastella sekä olemassa olevia tiedon keräämiseen liittyviä rikostunnusmerkistöjä että esitutkintaviranomaisten toimivaltuuksia ja näiden välistä epäsuhtaa. Rikostunnusmerkistöistä täsmentämistä saattaisivat uudessa toimintaympäristössä tarvita henkilörekisteririkos (RL 39:8) sekä maksuvälinepetoksen valmistelu (RL 37:11). Eräs mahdollisuus olisi myös identiteettitiedon – erityisesti etätunnistamiseen liittyvän identiteettitiedon – oikeudettoman kaappaamisen huomioiminen tunnusmerkistötekijänä rikoslain 34 luvun 9a §:ssä (Vaaran aiheuttaminen tietojenkäsittelylle).

Kohdassa 5.7.1. todetun lisäksi yksityiselle toisena esiintymisen kriminalisointia tulisi jatkoselvittää myös siksi, että yksityiselle ja viranomaiselle esiintyminen olisi kriminalisoitu samantasoisesti oikeusvaikutuksiltaan samantasoisissa tehtävissä.

Työryhmä ehdottaa jatkotyöryhmän perustamista, jossa oikeusministeriön johdolla tarkasteltaisiin tässä raportissa esille tuotujen ongelmien osalta rikoslain, perustuslain ja muiden tarvittavien säännösten toimivuutta ja lainsäädännön todellista vaikuttavuutta erityisesti uhrin asema huomioiden, jotta työ olisi valmis ennen mahdollista EU-sääntelyä vuonna 2012. Tässä yhteydessä työryhmä ehdottaa myös syyttäjälaitoksen kantojen selvittämistä.

5.7.4 Ennaltaehkäisy - tietoverkon identiteettivarkauksien toteutuskynnyksen kasvattaminen

Koska tietosuoja- ja esitutkintaviranomaisten rikostorjunnalliset keinot ovat tällä hetkellä rajalliset erityisesti tietoverkossa toteutetuissa teoissa, ennaltaehkäisy on erityisen keskeisessä roolissa identiteettivarkauksilla aiheutettujen vahinkojen torjunnassa. Keskeisiä kysymyksiä ovat tällöin:

a) Eri toimijoiden välinen yhteistyö
Työryhmä katsoo, että viranomaisten yhteistyön ja tietojenvaihdon tulisi olla suunnitelmallista ja sen tulisi turvata uhrin asemaa. Tietoa tulisi voida vaihtaa jatkuvasti operatiivisella tasolla laajapohjaisen asiantuntijakokoonpanon sisällä. Työryhmä ehdottaakin perustettavaksi identiteettiturvallisuuden neuvottelukunnan tätä tehtävää varten.

b) Yleisen tietoisuuden lisäämisen
Työryhmä katsoo, että yleistä tietoisuutta tulisi lisätä sekä identiteettitiedon väärinkäyttöön liittyvistä uhista että konkreettisista keinoista, joilla henkilö voi vähentää riskiä joutua identiteettivarkauden uhriksi. Palveluntarjoajien ja loppukäyttäjien tietoisuutta erilaisista nykyisistä ja uusista uhkatekijöistä sekä erilaisista varautumistavoista tulisi jatkuvasti lisätä erilaisin yhteisin toimenpitein.

5.8 Biometria

Biometristen tunnistusratkaisujen säädöstarve on ilmeinen. Julkishallinnon on myös muilla keinoin pyrittävä suojaamaan kansalaisten tunnistetietoja. Yksityissektoria on tiedotettava ja tarjottava heille turvallisia ratkaisuja, joissa riskit biometristen tietojen joutumisesta vääriin käsiin on minimoitu. Tämä on erityisen tärkeää biometrisen tiedon muuttumattomuuden vuoksi. Kerran menetettyä biometrista tietoa ei voida vaihtaa uuteen.

Lainsäädännön kehityksestä vastaa oikeusministeriö ja Valtioneuvoston periaatepäätöksen sähköisestä tunnistamisesta mukaisesti oikeusministeriö asettaa työryhmän selvittämään asiaa. Työryhmä pitää tämän työn saattamista loppuun erittäin tärkeänä.

Liite 1: Henkilökorttien myöntäminen EU-maissa

Kysymyspatteriston kysymykset

ULKOASIAINMINISTERIÖ HEL8008-90
Kansalaispalvelut
KPA-20 Eija Emtö 26.08.2009

Viite
HEL8008-79

Asia
EU-maiden henkilökorttikäytäntö; yhteenveto

Asiasanat	MATKUSTUSASIAKIRJAT
Hoitaa	**KPA-20**
Hoitaa UE	**ATE; BER; BRT; BRY; BUD; BUK; DUB; HAA; KOB; LIS; LJU; LON; LUX; MAD; NIC; PAR; PRA; RII; ROO; SOF; TAL; TUK; VAR; WIE; VIL**
Koordinoi	
Tiedoksi	KPA-10
	SM

Laatija jakanut

Oheisena yhteenveto, jossa edustustojemme vastaukset seuraaviin kysymyksiin:

1. Kuka myöntää henkilökortit asemamaassanne? Onko kyseessä viranomainen vai yksityinen toimija?

2. Keille henkilökortteja myönnetään, vainko omille kansalaisille vai myönnetäänkö myös ulkomaalaisille? Jos myönnetään ulkomaalaisille niin keille ulkomaalaisille?

3. Onko henkilökortti asemamaassanne pakollinen?

4. Mikä on asemamaanne henkilökorttien voimassaoloaika?

5. Kelpaavatko henkilökortit matkustusasiakirjoina ja jos kelpaavat niin missä valtioissa?

Kysely on tehty Sisäasiainministeriön poliisiosaston pyynnöstä.

LIITTEET 1 kpl sähköisesti

Lomakepohja: UH-Muistio

Kysymyspatteriston vastaukset 25.8.2009

Alankomaat

1. Alankomaissa henkilökortit myöntää henkilön asuinkunta.
2. Henkilökortit myönnetään vain Alankomaiden kansalaisille. Alankomaiden Maahanmuutto- ja kansalaistamisvirasto Immigratie- en naturalisatie Dienst (IND) myöntää ulkomaalaisille heidän oleskelustatustaan vastaavia lupakortteja, jotka ovat samalla henkilökortteja, mutta eivät matkustusasiakirjoja.
3. Henkilökortti ei ole pakollinen Alankomaissa, mutta jokaisen 14 vuotiaan ja sitä vanhemman henkilön on pystyttävä todistamaan henkilöllisyytensä viranomaisen sitä pyytäessä. Henkilöllisyys voidaan todistaa passilla, henkilökortilla, ajokortilla tai ulkomaalaiselle myönnetyllä oleskelulupa-/ henkilökortilla.
4. Alankomaiden henkilökortti on voimassa 5 vuotta.
5. Henkilökortit kelpaavat matkustusasiakirjoina 34 eurooppalaisessa valtiossa: Andorra, Belgia, Bulgaria, Espanja, Irlanti, Islanti, Iso-Britannia ja Pohjois-Irlanti, Italia, Itävalta, Kreikka, Kypros, Latvia, Liechtenstein, Liettua, Luxemburg, Malta, Monaco, Norja, Portugal, Puola, Ranska, Romania, Ruotsi, Saksa, San Marino, Slovakia, Slovenia, Suomi, Sveitsi, Tanska, Tsekki, Turkki, Unkari ja Viro.

Belgia

1. Belgiassa henkilökortit myöntää asuinkunnan väestörekisteriviranomainen. Kansallisella tasolla henkilökorttiasiat kuuluvat sisäministeriön hallinnonalaan.

2. Henkilökortti myönnetään kaikille Belgiassa laillisesti asuville, myös ulkomaalaisille.
3. Henkilökortti (tai passi) on Belgiassa pakollinen. Lain mukaan henkilöllisyystodistusta (henkilökortti tai passi) on kannettava aina mukana.
4. Henkilökortin voimassaoloaika on 5 vuotta. Alle 12-vuotialle myönnettävien henkilökorttien voimassaoloaika on 3 vuotta.
5. Henkilökortit kelpaavat matkustusasiakirjoina EU-maissa sekä Norjassa, Islannissa, Sveitsissä ja Liechtensteinissä.

Bulgaria

1. Henkilökortin voi myöntää Bulgariassa ainoastaan poliisi.
2. Henkilökortti myönnetään omille kansalaisille ja kolmannen maan kansalaisille. EU-kansalaisten osalta olemme kysyneet nootilla ja odotamme vastausta.

3. Henkilökortti on pakollinen 14 ikävuodesta alkaen ja sitä tulee pitää mukana rangaistuksen uhalla.

4. Henkilökortti on voimassa 10 vuotta.
5. Henkilökortti kelpaa matkustusasiakirjana EU-maissa. Vastaukset perustuvat suurlähetystön omiin tietoihin sekä puhelimitse saatuun informaatioon. Kysymykset on esitetty kirjallisesti Bulgarian ulkoministeriölle. Palaamme mikäli vastaus sisältää uutta tai yllä olevasta poikkeavaa tietoa.

Espanja

1. D.N.I.:t (Documento nacional de identidad, kansallinen henkilöllisyysdokumentti) myöntävät Policía Nacionalin (sisäministeriön alaisena toimiva kansallinen poliisi) henkilöllisyys-dokumenttitoimistot, joita on 44 koko maassa. Paikkakunnilla, joissa poliisin toimistoa ei ole, kiertävä yksikkö myöntää kortit tietyin väliajoin. Liikuntakyvyttömille tehdään kotikäynti hakemuksen vastaanottoa ja sormenjälkien ottoa varten läheisen pyynnöstä lääkärintodistuksella.
2. Kansallista henkilökorttia D.N.I. ei myönnetä ulkomaalaisille.
3. Pakollinen 14 vuotta täyttäneille Espanjassa oleskeleville espanjan kansalaisille, kortti on pidettävä aina mukana ja se on näytettävä viranomaisille sitä pyydettäessä. Kaikilla espanjalaisilla on oikeus saada kortti iästä tai asuinpaikasta riippumatta.
4. Jaoteltu seuraavasti:
   - Alle 30-vuotiaana haettu/uusittu kortti 5 vuotta.
   - Yli 30-vuotiaana uusittu kortti 10 vuotta.
   - Yli 60-vuotiaana uusittu kortti voimassa loppuelämän ajan.
   - Väliaikainen kortti (esim. vajailla hakupapereilla) voidaan myöntää vuodeksi erityistapauksissa.
5. Kelpaa matkustusasiakirjana seuraavissa maissa: Andorra, Belgia, Bulgaria, Englanti, Hollanti, Irlanti, Islanti, Italia, Itävalta, Kreikka, Kroatia, Kypros, Latvia, Liechtenstein, Liettua, Luxemburg, Makedonia, Malta, Monako, Norja, Portugali, Puola, Ranska, Romania, Ruotsi, Saksa, San Marino, Slovakia, Slovenia, Suomi, Sveitsi, Tanska, Tsekki, Unkari ja Viro.

Irlanti

Irlannissa ei myönnetä kansallisia henkilökortteja. Ainut poliisin myöntämä kortti on ns. Age Card, joka osoittaa henkilön olevan täyttänyt 18 vuotta olevan oikeutettu ostamaan alkoholia. Age Card'ia ei kuitenkaan hyväksytä muuhun tarkoitukseen korvaamaan normaalia henkilökorttia.

Iso-Britannia

Iso-Britannia ryhtyi myöntämään sirullisia henkilökortteja elokuussa 2009. Ensimmäiset henkilökortit myönnettiin eräille virkamiehille ja lokakuusta 2009 Manchesterin ja Citi of London lentokentän virkailijat voivat saada kortin vapaaehtoisuus pohjalta. Henkilökortti otetaan laajemmin käyttöön asteittain niin, että vuonna 2012 jokainen 16-

vuotias Iso-Britannian kansalainen (British Citizen, British subject) voi anoa henkilökorttia.

1. Iso-Britannian henkilökortin myöntää Home Office, Identity and Passport Service viranomainen. Korttia anotaan kuten passia, mutta henkilökortin saanti edellyttää henkilötietojen tallettamista National Identity rekisteriin.
2. Korttia voivat anoa kaikki Iso-Britannian kansalaiset (British citizens) ja maassa asumisoikeuden saaneet brittisyntyperää olevat kansalaiset (British subject). Henkilökortteja myönnetään kahtena versiona:
    - National Identity Card (tausta violetti/lohenpunainen), joka myönnetään rajoituksetta ja joka oikeuttaa matkustamisen ETA-alueella
    - Indentity Card (vaaleanpunainen/vihreä), joka myönnetään Iso-Britannian kansalaisille, joilla on oikeuden määräämiä matkustusrajoituksia. Henkilökortti voidaan eräissä tapauksissa antaa myös henkilöille, joilla on Iso-Britannian pysyvä oleskelulupa. Henkilökortti ei ole matkustuskelpoinen Iso-Britannian (ml. Kanaalin saaret ja Irlanti (Eire) ulkopuolella marraskuusta 2008 lähtien ETAn ulkopuolisille opiskelijoille ja Iso-Britannian kansalaisten kolmansista maista tuleville aviopuolisoille/partnereille on myönnetty ulkomaalaisten henkilökortti osoituksena oleskeluoikeudesta UKssa. Asteittain ulkomaalaisten henkilökortti tullaan antamaan kaikille maassa oleville ulkomaalaisille niin, että 2015 mennessä 90 %:lla ulkomaalaisista olisi oleskeluoikeuden osoittava henkilökortti.
3. Henkilökortin hankinta on Iso-Britannian kansalaisille vapaaehtoista.
4. Henkilökortin voimassaoloaika on 10 vuotta.
5. Vain National Identity Card on matkustuskelpoinen ETA-alueelle.

Italia

1. Henkilökortit myöntää se väestörekisteriviranomainen (Anagrafe - Servizi Demografici), jossa henkilö on kirjoilla. Italiassa myönnetään nykyään sekä vanhoja ns. paperisia henkilökortteja että uusia sähköisiä henkilökortteja (kuten suomalaiset hlökortit).
2. Matkustukseen oikeuttavia henkilökortteja myönnetään vain Italian kansalaisille. Italiassa kirjoilla oleville ulkomaalaisille voidaan myöntää henkilökortti, joka ei oikeuta matkustukseen
3. Henkilökortti ei ole pakollinen. Alle 16-vuotiaat saavat alaikäisen henkilökortin, joka ei oikeuta matkustamaan Suomeen, mutta kylläkin melkein kaikkiin muihin EU-maihin. Matkustukseen oikeuttava henkilökortti myönnetään 16-vuotta täyttäneille. Italian lain mukaan viranomaisen sitä vaatiessa henkilön täytyy pystyä todistamaan henkilöllisyytensä (hlökortti, passi, ajokortti, muulla tavoin).
4. Henkilökortti on voimassa 10 vuotta.
5. Italian kansalaiselle myönnetty henkilökortti käy matkustusasiakirjana EU-maissa ja eräissä muissakin maissa (ml. Albania, Egypti, Kroatia, Guadalupa, Martinique, Mauritius, Sveitsi, Tunisia, Turkki mutta näissä tapauksissa yleensä

vain matkanjärjestäjän kautta hankituilla ryhmämatkoilla). (vrt. myös kohta 3.)

Itävalta

1. Itävallassa henkilökortin myöntää kaupungista riippuen joko poliisi tai maistraatti. Jotkut kunnat ottavat vastaan henkilökorttihakemuksia ja ohjaavat nämä edelleen vastuullisille viranomaisille.
2. Henkilökortti myönnetään vain Itävallan kansalaisille.
3. Henkilökortti ei Itävallassa ole pakollinen.
4. Henkilökortti on voimassa 10 vuotta. Lapsille myönnetty henkilökortti on lapsen iästä riippuen voimassa kaksi (0-2-v.), viisi (2-12-v.) tai kymmenen vuotta (12-v.-)
5. Itävaltalainen henkilökortti käy matkustusasiakirjasta 36 eri maassa. Näitä ovat EU-maiden lisäksi Andorra, Islanti, Kroatia, Liechtenstein, Monaco, Montenegro, Norja, San Marino ja Sveitsi.

Kreikka

1. Henkilökortin myöntää vakituisen asuinpaikkakunnan paikallispoliisi.
2. Henkilökortti myönnetään ainoastaan Kreikan kansalaiselle.
3. Henkilökortti on pakollinen.
4. Henkilökortti myönnetään ensimmäistä kertaa 12 vuotta täyttäneelle kreikkalaiselle. Kortti on voimassa 15 vuotta. Kortti tulee kuitenkin uusia jos henkilön siviilisäädyssä tapahtuu muutoksia. Vanha henkilökortti tulee uusia, mikäli kortissa ei ole kansalaisuutta kirjoitettu latinalaisin kirjaimin.
5. Henkilökortti kelpaa matkustusasiakirjana EU-maissa.

Kypros

1. Henkilökortit Kyproksella myöntää sisäasiainministeriön kansalaisasioiden rekisteröinti- ja muutto-osasto (Civil registration and migration department).
2. Henkilökortti myönnetään
   - kyproslaisille
   - henkilöille, jotka ovat alkuperältään kyproslaisia
   - ulkomaalaisille, jotka oleskelevat laillisesti Kyproksella riippumatta siitä, onko heillä pysyvä vai väliaikainen oleskelulupa Kyproksella.
3. Henkilökortti on Kyproksella pakollinen henkilön täytettyä 12 vuotta.
4. Aikuisille, yli 18-vuotiaille myönnetään henkilökortti kymmeneksi vuodeksi, alaikäisille (12-18) viideksi vuodeksi
5. Kyproslaiselle henkilölle myönnetty Kyproksen henkilökortti kelpaa matkustusasiakirjana EU-maissa, ei kuitenkaan ulkomaalaiselle myönnetty.

Latvia

Latviassa ei vielä myönnetä kansalaisille henkilökortteja. Viranomainen, joka tulee vastaamaan henkilökorttien myöntämisestä, on sisäasiainministeriön alainen Kansalaisuus- ja maahanmuuttovirasto. Viraston mukaan kortteja aletaan myöntää aikaisintaan v. 2010-11.

Liettua

1. Henkilökorttihakemus jätetään asuinpaikkakunnan sisäasiainministeriön alaiselle maahanmuuttovirastolle, joka myös sen myöntää.
2. Henkilökortin saa vain Liettuan kansalainen.
3. Henkilökortti tai passi on Liettuassa pakollinen kaikille 16 vuotta täyttäneille. Alle 16 vuotiaallekin henkilökortti voidaan myöntää.
4. 16 vuotta täyttäneille henkilökortti myönnetään 10 vuodeksi ja alle 16 vuotiaille 5 vuodeksi.
5. Henkilökortti kelpaa matkustusasiakirjana EU-maissa ja lisäksi Islannissa, Montenegrossa, Kroatiassa, Makedoniassa, Norjassa, San Marinossa ja Sveitsissä.

Luxemburg

1. Henkilökortin myöntää asuinkunnan viranomainen.
2. Yli 15-vuotiaalle Luxemburgin kansalaiselle sekä alle 15-vuotiaille on tarkoitettu alaikäisen henkilökortti. Henkilön on myös asuttava Luxemburgissa.
3. Henkilökortti on pakollinen, jos ei ole voimassa olevaa passia.
4. Voimassaoloaika:
   - Yli 15-vuotiaan henkilökortti: 10 vuotta
   - 4-15-vuotiaan henkilökortti: korkeintaan 5 vuotta (voimassaoloaika rajattava 15-ikävuoteen asti)
   - 0-4-vuotiaan henkilökortti: korkeintaan 2 vuotta
5. Henkilökortti kelpaa matkustusasiakirjana EU-maissa sekä Sveitsissä.

Portugali

Portugalissa on voimassa olevia vanhan mallisia viranomaisten myöntämiä henkilökortteja (Bilhete de Identidade, B.I.). Näitä henkilökortteja on myönnetty Portugalin kansalaisille sekä Brasilian kansalaisille. Kortteja on myönnetty viideksi tai kymmeneksi vuodeksi kerrallaan. Brasilian kansalaiset ovat voineet saada henkilökortin edellyttäen että asuvat laillisesti maassa ja että heillä on Portugaliin oleskelulupa. Brasilialaisten oikeus saada henkilökortti perustuu Portugalin ja Brasilian väliseen kahdenkeskeiseen sopimukseen (Tratado Luso-Brasileiro, Porto Seguro vuodelta 2000/2003) ja vastavuoroisuuteen. Brasilian kansalaisille myönnetty henkilökortti on muuten samanlainen kuin

portugalilaisillekin myönnettävä henkilökortti, eroavaisuutena on ainoastaan maininta Brasilian kansalaisuudesta ja brasilialaisille myönnettävä kortti ei kelpaa matkustamiseen. Bilhete de Identidade kortteja ei enää myönnetä. Cartão de Cidadão ("kansalaisen kortti") korvaa B.I.:n ja tätä korttia on myönnetty jo noin kahden vuoden ajan. Viiteasiakirjan kysymyksiin 1.-5. on seuraavassa tämän kortin osalta vastaukset.

1. Kortit myöntää Portugalin viranomainen. Korttia voi hakea seuraavista viranomaistoimipaikoista:
   - Conservatória do Registo Civil, lähinnä Suomen maistraattia vastaava viranomainen, ja sen erilaiset toimipisteet
   - Portugalin suurlähetystöt ja konsulaatit ympäri maailmaa.
2. Cartão de Cidadão -kortti myönnetään Portugalin kansalaisille sekä ensimmäisessä kappaleessa selostetuissa tilanteissa myös Brasilian kansalaisille.
3. Henkilökortti on Portugalissa pakollinen kansalaisen täytettyä kuusi ikävuotta. Tämä pakko koskee niin Portugalissa kuin ulkomaillakin asuvia Portugalin kansalaisia.
4. Cartão de Cidadão -kortin voimassaoloaika on viisi vuotta.
5. Cartão de Cidadão -kortti kelpaa matkustusasiakirjana EU-maissa ja Schengen-alueella vain Portugalin kansalaisten osalta.

Puola

1. Henkilökortit (henkilötodistukset - dowód osobisty) myöntää pysyvän asuinpaikan mukainen virasto. Mikäli pysyvää asuinpaikkaa ei ole, henkilökorttia haetaan viimeisen pysyvän asuinpaikan virastosta. Erikoistapauksissa henkilökortin myöntää Varsovan Śródmieście-kaupunginosan kunnanvirasto (esim. ulkomailla syntyneelle puolalaiselle).
2. Henkilökortti myönnetään Puolan kansalaiselle, joka on täyttänyt 18 vuotta, mutta henkilökortti voidaan myöntää myös, mikäli henkilö on täyttänyt 15 vuotta ja yksi seuraavista ehdoista täyttyy:
   - hän käy töissä
   - hän ei asu vanhempiensa tai huoltaja/iensa kanssa
   - hänellä ei ole vanhempia tai huoltajaa

   Henkilökortti voidaan lisäksi myöntää vanhempien tai huoltajien anomuksesta henkilölle, joka ei ole täyttänyt 13 vuotta. Ulkomaalaiselle Puolasta pakolaisasemaa hakevalle henkilölle voidaan myöntää asiakirja (tymczasowe zaświadczenie tożsamości cudzoziemca), joka on osoitus henkilöllisyydestä ja luvasta oleskella Puolassa. Ulkomaalaisille kansalaisuudettomille henkilöille, sekä ilman huoltajaa oleville alaikäisille ulkomaalaisille, jotka ovat syntyneet Puolassa, voidaan myöntää henkilöllisyyden osoittava asiakirja (polski dokument tożsamości cudzoziemca).
3. Henkilökortti on Puolassa pakollinen.

4. Henkilökortti on voimassa 10 vuotta myöntämispäivästä. Poikkeukset: henkilökortti voi olla voimassa anomuksesta 65 vuotta täyttäneelle toistaiseksi ja 5 vuotta voimassa alle 18-vuotiaille.
5. Puolan henkilökortti kelpaa matkustusasiakirjana EU-maissa. Tämän lisäksi henkilökortti kelpaa matkustettaessa Bosniaan, Kroatiaan, Makedoniaan ja Hertsegovinaan. Alle 18-vuotiaat voivat käyttää henkilökorttia matkustaessaan. Puolassa ei vaadita lupaa vanhemmilta tai huoltajilta yksin matkustamiseen. Ulkomaalaiset tarvitsevat matkustamiseen ulkomaalaisille myönnettävän matkustusasiakirjan:
    - Puolassa pakolaisaseman saaneille myönnettävä asiakirja (dokument podróży)
    - matkustusasiakirja (polski dokument podróży dla cudzoziemca), jonka haltijan kansalaisuus ei ole Puolan.

Ranska

1. Henkilökortin myöntävät Ranskan viranomaiset. Hakemus tulee jättää asuinpaikan kaupungintalolle (La Mairie) tai poliisiprefektuuriin. Asuinpaikan ollessa ulkomailla hakemus tehdään konsulaatin kautta.
2. Henkilökortin myöntäminen edellyttää Ranskan kansalaisuutta, joten sitä ei myönnetä ulkomaalaisille.
3. Ranskassa henkilökortti ei ole pakollinen.
4. Voimassaoloaika on 10 vuotta.
5. Henkilökortti kelpaa matkustusasiakirjana EU- ja Schengen-maissa. Tämän lisäksi henkilökortti kelpaa matkustusasiakirjana tietyin edellytyksin joissakin maissa. Tiedustelut kyseisen maan konsulaatista.

Romania

1. Henkilökortit myöntävä viranomainen on poliisi (Romanian kansalaisille) ja Ulkomaalaisviranomainen, Autoritarea pentru Straini', joka myöntää henkilökortit Romanian kansalaisen ulkomaalaisille perheenjäsenille.
2. Henkilökortteja myönnetään Romanian kansalaisille, jotka ovat täyttäneet 14 vuotta ja joilla on kotipaikka Romaniassa. Niitä myönnetään myös Romanian kansalaisen ulkomaalaiselle perheenjäsenelle (EU-kansalaisen perheenjäsenen oleskelulupa tai EU-kansalaisen perheenjäsenen pysyvä oleskelulupa). Henkilökortteja myönnetään myös ulkomaalaisille, jotka työskentelevät Romaniassa pidempään kuin 90 päivää.
3. Henkilökortti on pakollinen.
4. Henkilökortin voimassaoloaika romanialaisille on 10 vuotta. EU-kansalaisen perheenjäsenen oleskelulupa on voimassa viisi vuotta ja EU-kansalaisen perheenjäsenen pysyvä oleskelulupa on voimassa 10 vuotta. Romaniassa työskentelevän ulkomaalaisen henkilökortti on voimassa työsopimuksen voimassaoloajan.

5. Henkilökortti käy matkustusasiakirjana EU-maissa.

Ruotsi

1. Ruotsissa henkilökortteja myöntää pääsääntöisesti poliisi, verotoimisto (Skatteverket) ja eri pankit. Joissain tapauksissa myös tietyt työnantajat (esim. Kronofogden ja landstinget) myöntävät työntekijöilleen henkilökortteja.
2. Ruotsin poliisi myöntää henkilökortteja ainoastaan omille kansalaisilleen, verotoimisto Ruotsin kansalaisille sekä maassa pysyvästi asuville ulkomaalaisille (käytäntö alkoi vasta 1.6.2009) ja pankit omille asiakkailleen. Pankit ovat viime aikoina kuitenkin tuntuvasti kiristäneet käytäntöjään henkilökorttien myöntämisessä maassa asuville ulkomaalaisille ja jotkut pankit ovat luopuneet henkilökorttien myöntämisestä kokonaan.
3. Henkilökortti ei ole pakollinen ja monet käyttävätkin sen sijasta ajokorttia. Ruotsissa asuva tarvitsee yleensä kuitenkin jokapäiväisen elämänsä helpottamiseksi joko henkilökortin tai ajokortin. Kummassakin on ruotsalainen henkilötunnus, mikä on välttämätön viranomaisten ja pankkien kanssa asioitaessa sekä esim. korttiostosten yhteydessä henkilöllisyyden varmentamiseen, ellei asiakkaalla ole käytössä henkilökohtaista tunnuslukua maksukorttiinsa.
4. Henkilökorttien yleisin voimassaoloaika on 5 vuotta (esim. Ruotsin poliisin, verotoimiston ja pankkien henkilökortit).
5. Ainoastaan poliisin myöntämää henkilökorttia voi käyttää matkustusasiakirjana Ruotsin ulkopuolella. Sillä voi matkustaa Schengen-alueella. Pohjoismaan kansalaiset voivat Pohjoismaissa matkustaessaan todistaa henkilöllisyytensä yleensä myös ajo- tai henkilökortilla.

Saksa

1. Henkilökortit Saksassa myöntää sen paikkakunnan rekisteriviranomainen = Einwohnermeldeamt, missä henkilö on kirjoilla tai missä hänellä on 1. asuinpaikka.
2. Henkilökortit myönnetään vain Saksan kansalaisille.
3. Kaikilla 16 vuotta täyttäneillä Saksan kansalaisilla pitää olla joko henkilökortti tai passi. Myös alle 16 vuotiaille voi hankkia henkilökortin, mikäli vanhemmat sen haluavat.Lapsille on olemassa myös Kinderpass. Se myönnetään lapsille 12 ikävuoteen saakka ja on voimassa korkeintaan 6 vuotta.
4. Alle 24 vuotiaille myönnettyjen henkilökorttien voimassaoloaika on 6 vuotta ja 24 vuotta täyttäneiden henkilökortti on voimassa 10 vuotta.
5. Saksan henkilökortti kelpaa matkustusasiakirjana kaikkiin EU-maihin, sekä Sveitsiin, Liechtensteiniin ja San Marinoon. (Muiden maiden kohdalla Saksan viranomaisten suositus on ennen matkaa selvittää asia sen maan suurlähetystön kanssa, minne matka kohdistuu, riittääkö henkilökortti vai pitääkö olla passi.)

Slovakia

1. Henkilökortit Slovakiassa myöntää poliisi (sisäministeriön alainen).
2. Henkilökortti myönnetään jokaiselle yli 15-vuotiaalle Slovakian kansalaiselle, jolla on vakinainen kotipaikka Slovakiassa. Pysyvästi maassa kirjoilla olevat ulkomaalaiset saavat myös omanlaisensa henkilökortin.
3. Henkilökortti on pakollinen.
4. Henkilökortin voimassaoloaika on 10 vuotta kerrallaan. Yli 60-vuotiailla ei ole voimassaoloaikaa. Ulkomaalaisille myönnettävien henkilökorttien voimassaoloaika riippuu maassaoloajasta.
5. Slovakian kansalaisten henkilökortti käy matkustusasiakirjana EU-Shengen alueella ja Kroatiassa.

Slovenia

1. Sloveniassa on yhteensä 58 itsenäistä, valtiotason hallinnollista yksikköä jotka myöntävät henkilökortteja. Hätätapauksissa myös sisäasiainministeriö voi myöntää henkilökortteja. Mikäli henkilö on ulkomailla, eikä pysty matkustamaan Sloveniaan, on teoriassa mahdollista että myös Slovenian edustustot voivat myöntää henkilökortteja. Edustustojen osalta toimintatapa ei kuitenkaan ole vakiintunut.
2. Henkilökortteja myönnetään Slovenian kansalaisille sekä ulkomaalaisille seuraavasti. Pysyvän oleskeluluvan saaneille täysi-ikäisille henkilöille myönnettävien henkilökorttien voimassaoloaika on kymmenen vuotta. Hakemus tulee jättää 30 päivän kuluessa pysyvän oleskeluluvan myöntämisestä. Tilapäisen oleskeluluvan saanut täysi-ikäinen henkilö voi halutessaan hakea henkilökorttia, jolloin henkilökortti voidaan myöntää tilapäisen oleskeluluvan keston ajaksi. Lisäksi mikäli ulkomaalaisella ei ole passia, hänelle voidaan myöntää väliaikainen henkilökortti yhdeksi vuodeksi. Myös 15 vuotta täyttäneille, pysyvän tai väliaikaisen oleskeluluvan omaaville, ulkomaalaisille voidaan hakemuksesta myöntää henkilökortti, mutta niiden voimassaoloaika ei voi ylittää viittä vuotta. Ulkomaalaisille myönnettävä henkilökortti (the identity card for aliens) poikkeaa slovenialaisille myönnettävästä.
3. Ei, ainoastaan siinä tapauksessa ettei henkilöllä ole muuta kuvallista henkilötodistusta.
4. 18 vuotta täyttäneillä henkilökortin voimassaoloaika on kymmenen vuotta, 3-18-vuotiailla henkilökortin voimassaoloaika on viisi vuotta ja 0-3-vuotiailla kolme vuotta. Mikäli henkilö kadottaa henkilökorttinsa kolmannen kerran, myönnetään hänelle seuraavaksi ainoastaan yhden vuoden voimassaoleva henkilökortti. Yhden vuoden voimassaolevan väliaikaisen henkilökortin jälkeen on kuitenkin mahdollista myöntää jälleen normaali henkilökortti. Yhden vuoden voimassaoleva henkilökortti myönnetään niille ulkomaalaisille, joiden oleskelulupaprosessi on kesken. Muiden ulkomaalaisille myönnettävien henkilökorttien osalta ks. kohta 2.

5. Slovenialaiset henkilökortit kelpaavat matkustusasiakirjoina EU- ja ETA-alueilla, Kroatiassa, Montenegrossa, Bosnia ja Hertsegovinassa sekä Makedoniassa.

Tanska

Tanskassa ei myönnetä kansallisia henkilökortteja. Kunnissa myönnetään 16-vuotta täyttäneille nuorille ID-KORT FOR UNGE - henkilökortti, joka on tarkoitettu käytettäväksi silloin, kun nuorten tulee voida osoittaa ikänsä ostaessaan alkoholia tai tupakkatuotteita.

Tsekki

1. Henkilökortit myöntää Tšekissä hakijan vakinaisesta kotipaikasta riippuen kaupungin- tai kunnanvirasto tai maistraatti.
2. Henkilökortti on pakollinen kaikille yli 15-vuotiaille Tšekin kansalaisille, joilla on vakinainen kotipaikka maassa. Henkilökortteja ei myönnetä ulkomaalaisille.
3. ks. kohta 2.
4. 4.15–20 -vuotiaille myönnetään henkilökortti viideksi vuodeksi ja yli 20-vuotiaille kymmeneksi vuodeksi. Väliaikaisia henkilökortteja, jotka ovat kuvallisia, mutta eivät koneellisesti luettavia, voidaan myöntää myös yhdeksi kuukaudeksi kortin häviämisen, vahingoittumisen tai tuhoutumisen johdosta tai yhdeksi vuodeksi esimerkiksi luonnonkatastrofin aiheuttamassa poikkeustapauksessa tai lähestyvien vaalien vuoksi.
5. Henkilökortit kelpaavat matkustusasiakirjoina EU-maissa.

Unkari

1. Unkarissa henkilökortin myöntävät paikalliset valtion rekisterivirastot (területi okmányiroda) ja Budapestin Keskusrekisterivirasto.
2. Kaikenikäisten Unkarissa asuvien Unkarin kansalaisten tulee hakea henkilökorttia, mikäli heillä ei ole voimassaolevaa passia tai kortin muotoista ajokorttia. Oleskeluluvan tai ns. sijoittautumisluvan haltijoiden, pakolaisten ja henkilöiden, joilla on oikeus toissijaiseen suojeluun, tulee hakea pysyvää henkilökortti
3. Jokaisella kansalaisella tulee olla yksi virallinen henkilöllisyystodistus, joka voi olla joko henkilökortti, passi tai kortin muotoinen 01.01.2001 jälkeen myönnetty ajokortti. Henkilökortti ei siten ole Unkarissa pakollinen.
4. Pysyvän henkilökortin voimassaoloaika on myöntämispäivämäärästä laskettuna
   - vuotta, jos henkilö on alle 6-vuotias,
   - vuotta, jos henkilö on 6–20-vuotias,
   - 10 vuotta, jos henkilö on yli 20-vuotias
5. Unkarin EU-hun liittymispäivästä (01.05.2004) lähtien Unkarin kansalaiset saavat matkustaa unionin jäsenmaihin ennen 01.04.1991 myönnetyllä henkilötodistuksella (kovakantinen, jossa on tasavallan vaakuna), 01.01.2000 jälkeen myön-

netyllä henkilökortilla (kortin muotoinen, muovinen) ja 01.01.2000 jälkeen myönnetyllä väliaikaisella henkilökortilla. Uudentyyppinen, kortin muotoinen henkilökortti kelpaa matkustusasiakirjana myös Kroatiaan ja Sveitsiin matkustettaessa. Ulkomaalaiselle myönnettävä henkilökortti ei käy matkustusasiakirjana. Ulkoministeriön konsuliosaston mukaan henkilökortin ottamisesta Unkarin edustustoissa myönnettävien matkustusasiakirjojen piiriin ei ole keskusteltu virallisesti. Näin ollen ei ole tietoa siitäkään, millä aikataululla tämä olisi lainsäädännöllisesti tai teknisesti mahdollista.

Viro

1. Virossa henkilökortteja myöntää sisäministeriön kansalaisuus- ja maahanmuuttovirasto (Kodakondsus- ja migratsiooniamet).
2. Henkilökortti myönnetään
   - Viron kansalaisille
   - ulkomaalaisille - myöntöperusteena on voimassaoleva oleskelulupa tai EU-kansalaisen oleskeluoikeuden rekisteröinti
   - kansalaisuudeton - myöntöperusteensa on voimassaoleva väliaikainen oleskelulupa.
3. Henkilökortti on pakollinen Viron kansalaiselle ja Virossa pysyvästi asuvalle ulkomaalaiselle.
4. Voimassaoloaika on maksimissaan 5 vuotta.
5. Henkilökortti kelpaa matkustusasiakirjana Viron kansalaiselle EU-maissa ja Euroopan talousalueella sekä Sveitsissä sekä EU:n kansalaiselle EU-maissa ja Euroopan talousalueella sekä Sveitsissä.

Liite 2: Liikenne- ja viestintäministeriön lausuma

Sulkulistapalvelu

Työryhmä ehdottaa loppupäätelmissään ajokorttien, henkilökorttien ja passien sulkulistapalvelun toteuttamismahdollisuuden selvittämistä. Toimenpiteen merkitystä identiteettivarkauksien estämiseksi on syytä korostaa. Raportissa painotetaan useaan otteeseen näiden poliisin myöntämien asiakirjojen turvallisuutta ja niiden merkitystä koko identiteetin hallinnan järjestelmälle. Kyseisten asiakirjojen avulla voidaan luoda johdannaisia asiakirjoja, kuten maksu- ja tunnistusvälineitä. Näiden johdannaisten asiakirjojen osalta on luotu tarkat järjestelmät siitä, kuinka niiden sulkeminen tai käytön estäminen toteutetaan niiden joutuessa pois oikealta haltijaltaan. Siksi onkin erikoista, että poliisin myöntämien laajalti tunnistamisessa käytettävien asiakirjojen osalta vastaavaa järjestelmää ei ole olemassa yksityisen puolen käyttöön. Asia on pitkälti sisäasiainministeriön ja Poliisihallituksen omin toimin edistettävissä, ja siinä tulisi ryhtyä pikaisiin toimenpiteisiin. Vastaavia sulkulistapalveluja on jo monissa maissa. Sulkulistan tulisi olla ainakin kaikkien poliisin myöntämien henkilöllisyyttä osoittavia asiakirjoja hyödyntävien palveluntarjoajien, kuten kauppojen, pankkien ja tunnistuspalvelun tarjoajien käytettävissä.

Käsitteet

Työryhmän pyrkimystä terminologian vakiinnuttamiseen alueella on niin ikään syytä korostaa. Erityisesti käsitykset henkilöllisyyden syntymisestä ja siitä, että ihmisellä voi olla ainoastaan yksi henkilöllisyys mutta useita identiteettejä etenkin sähköisessä maailmassa, ovat tärkeitä.

Identiteettivarkauksista

Identiteettivarkauksien merkitys nousee jatkuvasti esille alan toimijoiden keskuudessa. Toistaiseksi niiden uhrien määrä ei ole ollut hälyttävän suuri, mutta seuraukset yksilötasolla voivat olla hyvinkin vakavia. Jatkossa identiteettivarkauksien määrä voi nousta huomattavastikin, ja siksi on tärkeää ryhtyä ripeisiin toimiin niiden ehkäisemiseksi ja seurausten minimoimiseksi. Erityisen tärkeää on sulkea lainsäädäntöön ja erilaisiin käytänteisiin liittyvät aukot, joita voidaan pyrkiä käyttämään hyväksi. Työryhmän loppupäätelmät siitä, että työtä on edelleen jatkettava, ovat siksi oikeaan osuvia.

Yksityiskohtien osalta on todettava, että työryhmän raportin identiteettivarkauksiin liittyvät osiot 3.6 ja 4.5 on laadittu poliisiorganisaation toimesta, ja niissä tarkastellaan asiaa varsin puhtaasti poliisin toiminnan ja sitä sääntelevien lakien näkökulmasta. Esimerkiksi muun lainsäädännön mahdollisesti tarjoamia mahdollisuuksia ei raportissa ole varsinaisesti huomioitu. Lisäksi toimintaympäristö on jatkuvassa muutoksessa. Erityisesti on syytä mainita pakkokeinolain, esitutkintalain, poliisilain ja eräiden muiden lakien muuttamista koskeva hallituksen esitys, joka on parhaillaan eduskuntakäsittelyssä.

Kyseisten lakien muutoksissa on kyse useista sellaista seikoista, jotka saattavat vaikuttaa raporttiluonnoksessa esitettyihin arvioihin identiteettivarkauksien kriminalisointiin ja selvittämiseen liittyvistä ongelmista. Tätä analyysia ei ole voitu aikataulusyistä perusteellisesti tehdä. Edellä sanotun johdosta on tärkeää, että jatkotyössä oikeusministeriön johdolla käydään perusteellisesti läpi kaikki identiteettivarkauksiin liittyvät näkökohdat.

Työryhmän ehdottaman ”identiteettiturvallisuuden neuvottelukunnan” kokoonpano ja tehtävänanto ovat toistaiseksi määrittelemättä. Liikenne- ja viestintäministeriö varaa mahdollisuuden lausua näistä seikoista myöhemmässä vaiheessa.

Kansalaisvarmenne

Kansalaisvarmenteen osalta raportin johtopäätöksissä todetaan, että kansalaisvarmenteen tulevaisuus tullaan ratkaisemaan vuoden 2011 aikana valtiovarainministeriön johtamassa työryhmässä. Tämä toteamus pitää täysin paikkansa, mutta sen kanssa ristiriidassa on kohdassa 4.4 ”Kansalaisvarmenne ja tulevaisuuden käyttömuodot” sekä kohdan 5.1 viimeisessä kappaleessa esitetty. Kyseiset kohdat kuvaavat sisäasiainministeriön käsitystä asiassa, eikä kyseessä ole työryhmässä luotu teksti. Kohdissa esitetty on ristiriidassa myös sen kanssa, mitä raportissa on aikaisemmin todettu vahvasta sähköisestä tunnistamisesta.

Suomessa on ensimmäisenä maana maailmassa olemassa selkeä vahvan sähköisen tunnistamisen infrastruktuuri. Se on luotu kohdassa 3.5 kuvatun vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain avulla. Vahvan sähköisen tunnistamisen palveluita tarjoavat palveluntarjoajat ovat tehneet lain 10 §:ssä edellytetyt ilmoitukset Viestintävirastolle, ja Viestintäviraston internetsivuilta on löydettävissä rekisteri, joka sisältää tiedot näistä palveluntarjoajista. Ilmoituksen ovat tehneet kaikki Tupas-palveluita tarjoavat pankit, Väestörekisterikeskus sekä teleyritykset TeliaSonera Finland Oyj, Elisa Oyj ja DNA Oy. Viimeksi mainittujen palveluntarjoajien tunnistusvälineet ovat tulleet markkinoille 30.11.2010.

Mainittu laki perustuu sähköisen tunnistamisen kehittämisryhmän syksyllä 2008 laatimiin ja Arjen tietoyhteiskunnan neuvottelukunnan hyväksymiin vahvan sähköisen tunnistamisen kansallisiin linjauksiin, jotka on esitelty raportissa niin ikään kohdassa 3.5. Sisäasiainministeriö on ollut mukana yhteistyössä valmistelemassa niin lakiehdotusta kuin kansallisia linjauksiakin.

Kansallisissa linjauksissa todetaan muun muassa, että yksityisen ja julkisen sektorin palveluntarjoajat hankkivat tarvitsemansa sähköisen tunnistamisen palvelut toimivilta vahvan sähköisen tunnistamisen palveluiden markkinoilta. Samoin linjauksissa todetaan, että vahva sähköinen tunnistaminen soveltuu lähtökohtaisesti kaikkeen luotettavaan sähköiseen tunnistamiseen niin yksityisellä kuin julkisellakin sektorilla. Tähän ei siis tarvita valtion tarjoamaa varmennetta.

Luotettavan tunnistamisen mahdollistama infrastruktuuri on tosiaan syytä tunnustaa yhdeksi tietoyhteiskunnan perusinfrastruktuureista. Jo lähitulevaisuudessa on syytä olettaa, että sähköisten palveluiden määrä ja kirjo kasvavat, ja mitä kehittyneemmästä palvelusta on kysymys, sitä todennäköisemmin se tarvitsee luotettavaa eli vahvaa sähköistä tunnistamista toimiakseen riittävän turvallisesti. Myös julkisen sektorin palvelut siirtyvät yhä enenevässä määrin sähköisesti saataville, ja monet niistä voivat hyödyntää vahvaa sähköistä tunnistamista. Mutta kuten muunkaan tietoyhteiskunnan infrastruktuurin, myöskään tunnistamisinfrastruktuurin ei tarvitse olla valtion tarjoamaa. Esimerkiksi sellaisten tietoyhteiskunnan perusedellytysten kuin internetyhteyden tai puhelinliittymän saadakseen henkilön on solmittava sopimus yksityisen palveluntarjoajan kanssa, eikä tätä pidetä millään tavalla ongelmallisena.

Myöskään sähköisten allekirjoitusvälineiden tarjoamiseksi ei tarvita valtion tarjoamia palveluita. Kuten vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain 5.2 §:ssä todetaan, oikeustoimien tekemiseen Suomessa tarvitaan sähköistä allekirjoitusta ainoastaan hyvin harvoin. Jatkossa sähköisten allekirjoitusten merkitys saattaa kasvaa erityisesti viestinvälityksessä, sillä niiden avulla voidaan varmistaa, ettei lähetettyä asiakirjaa ole muutettu asiattomasti. Markkinoilla tarjottavat palvelut tulevat kuitenkin pitämään huolen myös tästä osasta palvelupalettia, mikäli sen käyttämiselle on jatkossa aito tilaus. Esimerkiksi markkinoille tulossa olevilla mobiilivarmenteilla voidaan tehdä sähköisiä allekirjoituksia.

Biometria

Raportin rakenne on sikäli poikkeuksellinen, että se sisältää osioita, jotka edustavat ainoastaan sisäasiainministeriön tai sen hallinnonalan näkemyksiä. Vaikka kohdat on pyritty merkitsemään, saattaa osittain jäädä epäselväksi, edustaako jokin näkökanta koko työryhmän vai ainoastaan sen osan näkemyksiä. Myös biometriaa koskettelevien osioiden 3.7 ja 4.6 osalta on syytä todeta, että niiden sisältämää tekstiä ei ole käsitelty työryhmän varsinaisen kokoonpanon kokouksissa.

Ulkomaalaisia koskevat raportin osuudet

Kuten raportin alussa todetaan, ulkomaalaisiin liittyviä asioita on käsitelty erillisissä kokouksissa. Niiden kokoonpano on poikennut työryhmän varsinaisesta kokoonpanosta. Liikenne- ja viestintäministeriön edustaja ei ole osallistunut näihin kokouksiin eikä raportin ulkomaalaisiin liittyvien osioiden valmisteluun.