EUROOPAN TIETOSUOJAVALTUUTETTU

Euroopan tietosuojavaltuutetun lausunto ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi diplomaatti- ja konsuliedustustoille annetun yhteisen konsuliohjeiston muuttamisesta biometristen tunnisteiden käyttöönoton ja viisumihakemusten vastaanoton ja käsittelyn järjestämistä koskevien määräysten osalta (KOM(2006) 269 lopullinen) — 2006/0088 (COD)

(2006/C 321/14)

EUROOPAN TIETOSUOJAVALTUUTETTU, joka

ottaa huomioon Euroopan yhteisön perustamissopimuksen ja erityisesti sen 286 artiklan,

ottaa huomioon Euroopan unionin perusoikeuskirjan ja erityisesti sen 8 artiklan,

ottaa huomioon yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY,

ottaa huomioon yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 45/2001 ja erityisesti sen 41 artiklan,

ottaa huomioon 19. kesäkuuta 2006 komissiolta saamansa asetuksen (EY) N:o 45/2001 28 artiklan 2 kohdan mukaisen lausuntopyynnön,

ON ANTANUT SEURAAVAN LAUSUNNON:

1. **JOHDANTO**

Asetusehdotuksella on kaksi pääasiallista tavoitetta, jotka molemmat liittyvät viisumitietojärjestelmän (VIS) täytäntöönpanoon:

— luoda jäsenvaltioille oikeudellinen perusta, jonka nojalla ne voivat ottaa pakolliset biometriset tunnisteet viisuminhakijoilta;

— asettaa oikeudelliset puitteet jäsenvaltioiden konsulaattien organisoinnille, erityisesti organisoimalla jäsenvaltioiden välistä mahdollista yhteistyötä viisumihakemusten käsittelyssä.

Näihin kahteen tavoitteeseen liittyy erilaisia tietosuojakysymyksiä, joten niitä käsitellään erikseen, vaikka ne kuuluvatkin samaan ehdotukseen.

Tarkasteltavana olevalla ehdotuksella pyritään muuttamaan yhteistä konsuliohjeistoa, jonka 14 päivänä kesäkuuta 1985 tehdyn Schengenin sopimuksen soveltamisesta tehdyllä yleissopimuksella perustettu toimeenpaneva komitea taannoin hyväksyi. Konsuliohjeisto on osa Schengenin säännöstöä, ja se sisällytettiin EU:n lainsäädäntöön Amsterdamin sopimuksen liitteenä olevalla pöytäkirjalla. Sitä on sen jälkeen muutettu useasti. Vaikka jotkin muutoksista ovat edelleen luottamuksellisia, yhteinen konsuliohjeisto julkaistiin vuonna 2000. Sisällöltään konsuliohjeisto on ennen kaikkea käsikirja, jossa on käytännön sääntöjä siitä, miten lyhytaikainen viisumi myönnetään. Siinä on säännöksiä mm. hakemusten tutkimisesta, päätöksenteosta ja siitä, miten viisumitarrat täytetään.

2. BIOMETRISTEN TUNNISTEIDEN KERÄÄMINEN

2.1 Alustava huomautus: biometristen tietojen erityispiirteet

Komission 28. joulukuuta 2004 esittämän VIS-ehdotuksen ([1]) mukaan jäsenvaltioiden on otettava käyttöön sormenjäljet ja valokuvat viisumitietojärjestelmään kuuluvina biometrisinä tunnisteina, joita käytetään todentamiseen ja (tai) tunnistamiseen. Tarkasteltavana olevalla ehdotuksella Euroopan parlamentin ja neuvoston asetukseksi yhteisen konsuliohjeiston muuttamisesta pyritään luomaan oikeudellinen perusta, jonka nojalla biometrisiä tunnisteita voidaan kerätä.

Euroopan tietosuojavaltuutettu antoi 23. maaliskuuta 2005 VIS-ehdotusta koskevan lausunnon ([2]). Tietosuojavaltuutettu korosti lausunnossa, kuinka tärkeää on, että biometristen tietojen erityslaadun vuoksi biometristen tietojen käsittelyssä on käytössä kaikki tarvittavat suojatoimet ([3]).

> *"Biometristen tietojen käyttö tietojärjestelmissä ei koskaan ole merkityksetön valinta eikä varsinkaan silloin, kun järjestelmä koskee valtavaa määrää henkilöitä. Biometriset tiedot (…) muuttavat peruuttamattomasti ruumiin ja henkilöllisyyden suhdetta, sillä biometristen tietojen avulla ihmisruumiin piirteistä tulee 'koneellisesti luettavia' mahdollista myöhempää käyttöä varten. Vaikka biometrisiä tietoja ei voi lukea ihmissilmällä, niitä voidaan lukea ja käyttää soveltuvilla välineillä milloin tahansa ja minne tahansa henkilö meneekin."*

Tietosuojavaltuutetun mukaan tämä biometristen tietojen arkaluonteisuus edellyttää, että velvoite käyttää biometrisia tietoja otetaan käyttöön vasta sen jälkeen, kun sen riskit on arvioitu perusteellisesti, ja että siinä olisi noudatettava menettelyä, jota voidaan täysin valvoa demokraattisesti. Nämä huomautukset ovat perustana tietosuojavaltuutetun tarkastellessa ehdotusta.

2.2. Ehdotuksen asiayhteys

Tämän ehdotuksen konteksti tekee siitä vielä arkaluonteisemman. Asetusehdotusta ei voida tarkastella erikseen, ottamatta huomioon muiden suurisuuntaisten tietotekniikkajärjestelmien kehittämistä ja yleistä suuntausta tietojärjestelmien väliseen entistä suurempaan yhteentoimivuuteen. Tämä on mainittu 24. marraskuuta 2005 päivätyssä komission tiedonannossa eurooppalaisten tietokantojen tehokkuuden parantamisesta, yhteentoimivuuden lisäämisestä ja synergioista oikeus- ja sisäasioiden alalla ([4]).

Näin ollen tietyssä kontekstissa ja tiettyä tarkoitusta varten tehty päätös todennäköisesti vaikuttaa muihin tarkoituksiin rakennettujen järjestelmien kehittämiseen ja käyttöön. Biometrisiä tietoja — todennäköisesti mukaan luettuina tiedot, jotka on kerätty viisumipolitiikan täytäntöönpanemiseksi — voidaan käyttää eri yhteyksissä sen jälkeen, kun ne ovat saatavilla. Tämä voisi koskea SIS-puitteiden lisäksi todennäköisesti myös Europolia ja Frontexia.

2.3. Velvollisuus antaa sormenjäljet

Tarkasteltavana olevan ehdotuksen perusteluissa todetaan seuraavaa: "Koska biometristen tunnisteiden ottaminen muodostaa osan viisuminhakumenettelyä, yhteistä konsuliohjeistoa on muutettava oikeudellisen perustan luomiseksi kyseiselle toimenpiteelle."

Tietosuojavaltuutettu vastustaa lainsäätäjän valintaa sisällyttää yhteiseen konsuliohjeistoon (pikemminkin kuin itse VIS-asetukseen) säännöksiä siitä, vapautetaanko tietyt henkilöt tai henkilöryhmät velvollisuudesta antaa sormenjäljet. Ensinnäkin säännöksillä on suuri vaikutus hyvin monien ihmisten yksityisyyteen, ja siksi ne kuuluisivat peruslainsäädäntöön eivätkä luonteeltaan lähinnä teknisiin ohjeisiin. Toiseksi, oikeudellisen järjestelmän selkeyden vuoksi olisi parempi käsitellä asia samassa tekstissä, jolla perustetaan itse tietojärjestelmä.

([1]) Ehdotus Euroopan parlamentin ja neuvoston asetukseksi viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta (KOM(2004) 835 lopullinen), jonka komissio esitti 28.12.2004.

([2]) Euroopan tietosuojavaltuutetun lausunto, annettu 23.3.2005 ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta, EUVL C 181, 23.7.2005, s. 13.

([3]) *"Biometriset tiedot ovat lähes täydellisen erottelevia, ts. jokaisella henkilöllä on ainutlaatuiset biometriset piirteet. Nämä piirteet eivät myöskään juuri koskaan muutu henkilön eliniän aikana, joten tiedot ovat pysyviä. Jokaisella on samat fyysiset 'tekijät', minkä ansiosta biometriset tiedot ovat universaaleja."* (ibid.).

([4]) KOM(2005) 597 lopullinen.

a) Ensinnäkin oikeusperustan luominen pakolliselle sormenjälkien ja muiden biometristen tunnisteiden ottamiselle on paljon enemmän kuin vain tekninen seikka: sillä on merkittävä vaikutus asianomaisten henkilöiden yksityisyyteen. Varsinkin ala- ja/tai yläikärajan määrittäminen sormenjälkien ottamiseksi on poliittinen päätös eikä vain tekninen. Sen vuoksi tietosuojavaltuutettu suosittaa, että tämä asia, varsinkin ne näkökohdat, jotka eivät ole puhtaasti teknisiä, käsiteltäisiin perustekstissä (VIS-asetusehdotuksessa) eikä käsikirjassa, joka sisältää lähinnä viisumimenettelyn teknisiä ja käytännön näkökohtia koskevia ohjeita ([1]).

Tältä osin on myös hyödyllistä palauttaa mieleen Euroopan ihmisoikeussopimuksen (ECHR) vaatimukset ja siihen liittyvä oikeuskäytäntö. ECHR:n 8 artiklan 2 kohdan mukaan viranomaiset eivät saa puuttua yksityisyyttä koskevan oikeuden käyttämiseen, paitsi "kun siitä on säädetty laissa" ja se on "välttämätöntä demokraattisessa yhteiskunnassa" merkittävien asioiden suojaamiseksi. Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä nämä ehdot ovat johtaneet lisävaatimuksiin, jotka koskevat asiaan puuttumisen oikeusperustan laatua (siitä on säädettävä saatavilla olevassa lainsäädännössä, ja sen on oltava ennakoitavissa), toimenpiteiden oikeasuhteisuutta sekä väärinkäytöltä suojaavien asianmukaisten suojatoimenpiteiden tarvetta.

On tosiasia, että tässä kuvattu osaratkaisuihin perustuva lainsäädäntöä koskeva lähestymistapa ei johda selkeään ja helposti saatavilla olevaan sääntelyyn, mutta voidaan pohtia sitäkin, kelpaako yhteinen konsuliohjeisto sinänsäkään. Kysymyksiä voi nousta esiin tekstin (mahdollisessa) tulevassa muuttamisessa käytettävästä menettelystä. Olisi joka tapauksessa taattava, että näin merkittävää päätöstä ei voida muuttaa ilman menettelyä, johon kuuluu asianmukainen avoimuus ja demokraattinen kuuleminen.

b) Toinen kysymys koskee oikeudellisen järjestelmän selkeyttä. Ehdotuksen perusteluista ei käy selväksi, miksi tarvitaan eri oikeudellinen perusta biometristen tunnisteiden keräämiselle ja niiden käsittelylle. Sen mukaan "tässä ehdotuksessa käsitellään biometristen tietojen keruuta, kun taas viisumitietojärjestelmää koskeva ehdotus kattaa tietojen siirtämisen ja vaihdon" ([2]). Tietosuojan kannalta henkilötietojen käsittely kuitenkin kattaa tietojen keräämisen. Samaan toimintaketjuun kuuluvien toimien sääntely eri oikeudellisissa teksteissä saattaa heikentää järjestelmän selkeyttä. Tämä on ongelma sekä rekisteröityjen (joita ehdotus koskee) että järjestelmän demokraattisen valvonnan kannalta. On yhä vaikeampaa saada kokonaiskäsitys tästä alasta, jolla eri säädökset sääntelevät pohjimmiltaan samaa tietojenkäsittelyä.

2.4. **Vapautukset sormenjälkien antamista koskevasta vaatimuksesta**

Tätä kuvaa hyvin kysymys eri henkilöluokista, jotka on vapautettu sormenjälkien antamista koskevasta velvollisuudesta (tähän kuuluvat erityisesti nuoret lapset).

Nuorten lasten sormenjälkien ottamisen sallittavuutta olisi käsiteltävä ottaen huomioon koko viisumitietojärjestelmän tarkoitus. Toisin sanoen VIS-ehdotuksen mukaisesti sen, että määrätään biometristen tunnisteiden ottamisesta joiltakin henkilöryhmiltä tai vapautetaan ne tästä velvollisuudesta, on oltava oikeasuhteinen toimenpide viisumipolitiikan ja sitä koskevien tavoitteiden puitteissa. Oikeasuhteisuutta olisi arvioitava demokraattisella menettelyllä.

Sitä olisi arvioitava myös sormenjälkien käyttötarkoituksen valossa, VIS-ehdotuksessa kuvatun mukaisesti. Biometriikkaa käytetään joko todentamiseen tai tunnistamiseen, ja biometristä tunnistetta voidaan pitää teknisesti sopivana yhteen näistä käyttötarkoituksista mutta ei toiseen. Alle 14-vuotiaiden lasten sormenjälkien käsittelyä pidetään yleensä luotettavana vain todentamiseen. Tämän pitäisi vaikuttaa ehdotuksen analyyttiseen tarkasteluun, mutta tarvittavat seikat löytyvät jälleen VIS-ehdotuksesta (ja niitä ei vielä ole päätetty).

Lopuksi voidaan todeta, että tietosuojavaltuutettu kehottaa painokkaasti, että VIS-ehdotuksessa esitettyjä poikkeuksia biometristen tunnisteiden ottamiseen säännellään tiukasti selkeyden ja johdonmukaisuuden vuoksi. Biometristen tunnisteiden ja tässä tapauksessa varsinkin sormenjälkien keräämisen sääntely olisi nähtävä liitännäissääntelynä pääasialliseen säädökseen nähden, ja siksi sitä olisi käsiteltävä itse pääasiallisessa asiakirjassa.

([1]) Erioikeusperustat (yhteinen konsuliohjeisto: 62 artiklan 2 kohdan b alakohdan ii alakohta; VIS-asetus: 66 artikla), eivät estä lainsäätäjää käsittelemästä asiaa samassa tekstissä.

([2]) Perustelut, s. 5.

2.5. **Viisuminhakijoiden ikä**

Ehdotuksen mukaan ainoastaan alle kuusivuotiaisiin lapsiin ei sovelleta sormenjälkien antamista koskevaa vaatimusta. Tämä herättää monia kysymyksiä (riippumatta siitä, tuleeko tämä säännös olemaan viisumitietojärjestelmää (VIS) vai yhteistä konsuliohjeistoa koskevassa ehdotuksessa).

Tietosuojavaltuutettu katsoo ensinnäkin, että yleistä sormenjälkien ottamista lapsilta ei voida nähdä ainoastaan teknisenä yksityiskohtana, vaan siitä tulisi käydä asiaankuuluvissa toimielimissä vakava demokraattinen keskustelu. Tällaisen päätöksen ei tulisi perustua vain tekniseen toteutettavuuteen, vaan myös ainakin siitä viisumitietojärjestelmän täytäntöönpanolle koituvaan etuun. Lukuun ottamatta eräitä hyvin harvoja jäsenvaltioita tästä asiasta ei kuitenkaan näytä olevan meneillään julkista keskustelua, mikä on hyvin valitettavaa.

Muistettakoon myös, että VIS perustetaan periaatteessa viattomien matkustajien (eli matkustajien pääosan) viisumimenettelyjen helpottamiseksi. Näin ollen mukavuuteen ja ergonomiaan liittyvät näkökohdat olisi otettava huomioon ([1]). Biometristen tunnisteiden käytön, tapahtui se viisumihakemusmenettelyn tai rajatarkastusten yhteydessä, ei pitäisi liikaa vaikeuttaa viisumimenettelyjen noudattamista lasten kohdalla.

Olisi myös muistettava, että kaikki biotunnistusjärjestelmät ovat teknisesti epätäydellisiä. Tieteellinen kirjallisuus ei anna lopullista näyttöä siitä, että luotettavan tunnistuksen voisi tehdä alle 14-vuotiaiden lasten sormenjälkien perusteella. Tähän mennessä ainoat laajapohjaiset tätä koskevat kokemukset on saatu Eurodac- ja US-Visit -järjestelmien käytöstä. Kiinnostavaa kyllä, kummassakin järjestelmässä lapsilta otetaan sormenjäljet 14 vuoden iästä lähtien. Tätä nuorempien lasten sormenjälkien ottamista tulisi perustella tutkimuksin, jotka osoittavat niiden tarkkuuden ja käyttökelpoisuuden viisumitietojärjestelmän kaltaisessa laajassa tietokannassa.

Joka tapauksessa on suositeltavaa käyttää nuorempien lasten sormenjälkiä vertaamalla yhtä yhteen kuin yhtä moniin. Tästä tulisi antaa nimenomainen säännös.

Tämän asian käsittelyn lopuksi todettakoon, että useimmat tehdyistä huomautuksista eivät koske vain lapsia, vaan myös aikuisia. Sormenjälkien tarkkuus ja käyttökelpoisuus vähenevät ihmisen ikääntyessä ([2]), ja mukavuuteen ja ergonomiaan liittyvät näkökohdat ovat myös erityisen tärkeitä.

2.6. **Valokuvat**

Samaa voitaisiin sanoa valokuvista, joiden käytölle ei tässä ehdotuksessa eikä VIS-ehdotuksessa ole asetettu mitään ikärajaa. Voidaan kuitenkin kysyä, ovatko lapsenkasvoisena otetut valokuvat todella käyttökelpoisia tunnistamiseen tai edes henkilöllisyyden varmistamiseen.

Lasten kasvontunnistus (oli se tulevaisuudessa automatisoitua tai ihmisten tekemää), joka perustuu muutaman vuoden takaisiin valokuviin, on todennäköisesti ongelmallista. Vaikka kasvontunnistustekniikka kehittyisi merkittävästi, on hyvin epätodennäköistä, että tietokoneohjelmat voivat lähitulevaisuudessa ennustaa kasvun vaikutukset lasten kasvoihin. Tästä syystä VIS-asetuksessa olisi täsmennettävä, että niin kauan kuin kasvontunnistustekniikka ei ole riittävän luotettavaa, valokuvia voidaan käyttää vain yksilöiden henkilöllisyyden varmentamisen tai heidän tunnistamisensa tukena, kun muistetaan, että lasten osalta tämä asiantila jatkunee kauemmas tulevaisuuteen.

Yleisesti ottaen tietosuojavaltuutettu suosittaa molempien biometristen tunnisteiden osalta, että harkittaisiin vakavasti sitä, painaako saatu hyöty (laittoman maahanmuuton ja lasten salakuljetuksen torjunta) enemmän kuin edellä mainitut varjopuolet.

2.7. **Muut poikkeukset**

Ehdotuksen mukaan hakijoihin, ”joiden sormenjälkien ottaminen on fyysisesti mahdotonta”, ei sovelleta sormenjälkien antamista koskevaa vaatimusta.

([1]) Tätä painotettiin Alankomaiden hallituksen tilaamassa tutkimuksessa: J.E. DEN HARTOGH et al., *How do you measure a child? A study into the use of biometrics in children*, 2005, TNO.

([2]) Ks. esim. A. HICKLIN ja R. KHANNA, *The Role of Data Quality in Biometric Systems*, MTS, 9.2.2006.

Tietosuojavaltuutettu on jo huomauttanut VIS-ehdotusta koskevassa lausunnossaan, että tämä tilanne koskee merkittävää henkilömäärää: on arvioitu, että väestöstä jopa 5 prosentin tietoja ei voisi rekisteröidä. Kun on kyse tietokannasta, johon kirjataan vuosittain 20 000 000 tiedot, tämä merkitsee, että tietojen rekisteröinti voisi vuositasolla tuottaa vaikeuksia jopa miljoonassa tapauksessa. Tämä olisi varmasti pidettävä mielessä tätä ehdotusta tarkasteltaessa. Lisäksi tietosuojavaltuutettu painotti toimivien varamenettelyjen tarvetta:

”olisi oltava käytettävissä varajärjestelmämenettelyjä, jotka ovat olennaisia suojatoimia biometristen tietojen käyttöönotossa, sillä ne eivät ole kaikkien käytettävissä eivätkä täysin tarkkoja. Tällaisia menettelyjä olisi otettava käyttöön ja käytettävä sellaisten henkilöiden huomioon ottamiseksi, joiden tietoja ei voida rekisteröidä normaalimenettelyin. On vältettävä tilanne, jossa nämä henkilöt joutuvat kärsimään järjestelmän puutteellisuuksista.”

Asetusehdotuksen mukaan viisumitietojärjestelmässä otetaan näissä tapauksissa käyttöön merkintä ”ei sovelleta”. Tämä on varmasti tarpeellista. Voidaan kuitenkin pelätä, että mahdottomuus rekisteröidä tietoja voisi helpommin johtaa viisumin epäämiseen. Jos hyvin korkea prosenttimäärä tapauksista, joissa rekisteröintiä ei ole voitu tehdä, johtaa viisumin epäämiseen, se ei ole hyväksyttävää.

Tästä syystä VIS-asetukseen olisi lisättävä säännös, jonka mukaan se, että tietoja ei voi rekisteröidä, ei saa automaattisesti johtaa viisumin myöntämistä koskevaan kielteiseen vastaukseen. Lisäksi VIS-asetuksen mukaisessa toimintaa koskevassa selvityksessä olisi erityisesti huolehdittava tästä asiasta: rekisteröinnin fyysiseen mahdottomuuteen liittyvää suurta evättyjen viisumien määrää tulisi seurata.

3. **VIISUMIHAKEMUSTEN ULKOISTAMINEN**

Jäsenvaltioiden (muun muassa laitteiston hankinta- ja ylläpitokuluista johtuvan) taakan keventämiseksi ehdotuksessa on useita mahdollisia yhteistyöjärjestelyjä:

— yhteisten tilojen järjestäminen: yhden tai useamman jäsenvaltion henkilökunta käsittelee hakemukset (myös biometriset tunnisteet), jotka sille on osoitettu toisen jäsenvaltion konsuli- ja diplomaattiedustustossa, ja jakaa välineistön kyseisen jäsenvaltion kanssa;

— yhteiset viisumikeskukset: kahden tai useamman jäsenvaltion diplomaattiedustustojen henkilökunta kootaan samaan rakennukseen sille osoitettujen viisumihakemusten (myös biometristen tunnisteiden) vastaanottamista varten;

— ehdotus sisältää myös mahdollisuuden, että ulkoinen palveluntarjoaja voisi ottaa viisumihakemuksen vastaan ja kerätä biometriset tunnisteet (tämä tuntuu olevan viimeinen vaihtoehto niille jäsenvaltioille, jotka eivät voi käyttää kumpaakaan kahdesta muusta mahdollisuudesta, vaikkakaan tämä ei ole aivan selvää).

Ehdotuksessa on nähty paljon vaivaa sen varmistamiseksi, että voidaan valita vain luotettavia ulkoisia palveluntarjoajia, ja että nämä palveluntarjoajat kykenevät varmistamaan, että ne toteuttavat kaikki tarpeelliset toimenpiteet tietojen suojaamiseksi ”vahingossa tapahtuvalta tai laittomalta tuhoamiselta, vahingossa tapahtuvalta häviämiseltä, muuttamiselta, luvattomalta luovuttamiselta tai käytöltä (…)” (ehdotuksen 1.B.2 kohta).

Tämä säännös on laadittu hyvin huolellisesti ja ottaen tietosuojan tarkoin huomioon, mihin tietosuojavaltuutettu on tyytyväinen. Viisumihakemusten käsittelyn antaminen kolmannessa maassa sijaitsevalle ulkoiselle palveluntarjoajalle aiheuttaa kuitenkin eräitä viisumin myöntämistä varten kerättyjen (joskus hyvin arkaluontoisten) tietojen suojaan liittyviä seurauksia.

Tietosuojavaltuutettu korostaa etenkin seuraavia seikkoja:

— kolmannen maan lainsäädännön tai käytäntöjen vuoksi saattaa osoittautua hyvin vaikeaksi, ehkä jopa mahdottomaksi tarkistaa työntekijöiden taustoja;

— vastaavasti ei ehkä ole mahdollista määrätä seuraamuksia yksityisyyttä koskevan lainsäädännön rikkomisesta ulkoisen palveluntarjoajan henkilöstölle (vaikka pääsopimuspuolelle voidaankin langettaa sopimusseuraamuksia);

— poliittiset levottomuudet tai muutokset voivat vaikuttaa yksityisyritykseen niin, että se ei pysty suoriutumaan käsittelyn turvallisuutta koskevista velvoitteistaan;

— tosiasiallinen valvonta voi olla vaikea toteuttaa, vaikka ulkoisten kumppanien kohdalla se olisi vielä tarpeellisempaa.

Näin ollen kaikkien ulkoisten palveluntarjoajien kanssa tehtyjen sopimusten olisi sisällettävä tietosuojan noudattamisen varmistamiseksi tarvittavat takeet, mukaan lukien ulkoiset tarkastukset, säännölliset satunnaistarkastukset, raportointi ja järjestelyt, jotta taattaisiin sopimuspuolen vastuu yksityisyyssääntöjen rikkomisen varalta, myös velvollisuus korvata henkilöille, jotka ovat kärsineet palveluntarjoajan toiminnasta johtuvaa vahinkoa.

Näiden huolenaiheiden lisäksi saattaa olla vielä tärkeämpää, että tiedostetaan se, että jäsenvaltiot eivät voi taata ulkoistetun tietojenkäsittelyn suojelua (eivätkä yhteisessä viisumikeskuksessa tapahtuvaa tietojenkäsittelyä, mikäli se tapahtuu diplomaattiedustuston ulkopuolisessa rakennuksessa) jotakin mahdollista asianomaisen maan viranomaisten toimenpidettä vastaan (esim. etsintä tai takavarikko) ([1]).

Ulkoista palveluntarjoajaa koskee kaikkien muiden sopimussäännösten lisäksi myös sen kolmannen maan kansallinen laki, johon se on sijoittunut. Viimeaikaiset tapahtumat, jotka koskevat kolmannen valtion viranomaisten pääsyä EU:ssa sijaitsevan yrityksen käsittelemiin rahoitusta koskeviin tietoihin osoittavat, että vaara on kaikkea muuta kuin teoreettinen. Tähän voisi lisäksi liittyä joidenkin kolmansien maiden kohdalla vakava yksilöihin kohdistuva vaara, jos valtio haluaa tietää, ketkä sen kansalaiset ovat hakeneet viisumia (poliittisten vastustajien ja toisinajattelijoiden valvomiseksi). Yksityisen yrityksen — useimmissa tapauksissa todennäköisesti paikallinen — henkilöstö ei pystyisi vastustamaan asianomaisten maiden hallitusten tai lainvalvontaviranomaisten harjoittamaa painostusta, jos nämä pyytäisivät heiltä tietoja.

Tämä on esitetyn järjestelmän suuri heikkous verrattuna siihen, että tiedot käsitellään konsuli- tai diplomaattiedustuston tiloissa. Siinä tapauksessahan tietoja suojellaan 18 päivänä huhtikuuta 1961 tehdyn diplomaattisia suhteita koskevan Wienin yleissopimuksen nojalla. Tämän yleissopimuksen 22 artiklassa määrätään näin:

> *”Edustuston tilat ovat loukkaamattomia. Vastaanottajavaltion edustajat eivät edustuston päällikön luvatta saa tunkeutua niihin. (…) Edustuston tilat, niiden kalustus ja muu niissä oleva omaisuus sekä edustuston kuljetusvälineet ovat vapautetut etsinnästä, pakko-otosta, takavarikoinnista tai täytäntöönpanotoimenpiteistä”.*

Lisäksi direktiivin 95/46/EY 4 artiklan 1 kohdan b alakohdan mukaan direktiivin kansallisia täytäntöönpanosäännöksiä sovelletaan tällaiseen henkilötietojen käsittelyyn, mikä osaltaan vahvistaa niiden suojelua.

Näin ollen vaikuttaa selvältä, että ainoa tehokas tapa suojella viisuminhakijoita ja heidän yhteyshenkilöitään (EU-kansalaisia tai -yrityksiä) koskevia tietoja on taata heille Wienin yleissopimuksen mukainen suoja. Tämä tarkoittaa, että tietoja tulisi käsitellä diplomaattisen suojelun piirissä olevissa tiloissa. Se ei estäisi jäsenvaltioita ulkoistamasta viisumihakemusten käsittelyä, mikäli ulkopuolinen sopimuspuoli voi toimia diplomaattisen edustuston tiloissa. Sama pätisi myös yhteisiin viisumikeskuksiin.

Tietosuojavaltuutettu vastustaa siis selkeästi ehdotuksen sivulla 15 uudessa 1.B.1.b) kohdassa olevaa mahdollisuutta ulkoistaa viisumihakemusten käsittely ja antaa se ulkoisille palveluntarjoajille. Tältä osin hyväksyttäviä vaihtoehtoja ovat:

— viisumihakemusten käsittelyn ulkoistaminen antamalla se yksityisyrityksen tehtäväksi, mikäli toiminta tapahtuu paikassa, joka on diplomaattisen suojelun alainen;

— ainoastaan tietojen antamisen ulkoistaminen puhelinpalvelukeskukselle 1.B.1.a) kohdassa esitetyn mukaisesti.

4. **PÄÄTELMÄT**

Tietosuojavaltuutettu on tyytyväinen siihen, että tämä yhteisen konsuliohjeiston muuttamista koskeva ehdotus on hyväksyttävä yhteispäätösmenettelyllä, mikä parantaa demokraattista valvontaa alalla, jossa sitä varmasti tarvitaan.

([1]) Tämä ongelma on jo olemassa matkatoimistojen käsitellessä hakemuksia; se muuttuu kuitenkin vielä arkaluontoisemmaksi, kun kyseessä ovat biometriset tiedot ja koska matkatoimiston käyttö ei ole periaatteessa pakollista.

Sisällöllisesti tietosuojavaltuutettu suosittaa seuraavaa:

— sormenjälkien antamisvelvoitetta koskevat poikkeukset olisi käsiteltävä pikemminkin VIS-asetuksessa kuin yhteistä konsuliohjeistoa koskevassa asetuksessa järjestelmän selvyyden ja johdonmukaisuuden varmistamiseksi;

— sormenjälkien ottamista ja valokuvia koskevia ikärajoja tulisi harkita tarkoin ottaen huomioon toteutettavuusnäkökohdat mutta myös eettiset sekä mukavuutta ja tarkkuutta koskevat seikat;

— valokuvia ei tulisi pitää yksinään riittävänä tunnistustapana vaan ainoastaan tunnistuksen tukena;

— viisumihakemusten käsittelyn ulkoistaminen yksityiselle yritykselle tulisi sallia vain, jos se tapahtuu diplomaattisen suojelun alaisissa tiloissa ja perustuu sopimussäännöksiin, jotka takaavat tehokkaan valvonnan ja sopimuspuolen vastuuvelvollisuuden.

Tehty Brysselissä 27. lokakuuta 2006

Peter HUSTINX

Euroopan tietosuojavaltuutettu