EUROOPAN TIETOSUOJAVALTUUTETTU

Euroopan tietosuojavaltuutetun lausunto

— ehdotuksesta neuvoston päätökseksi toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä (KOM (2005) 230 lopullinen);

— ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä (KOM (2005) 236 lopullinen) ja

— ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi ajoneuvojen rekisteröintitodistusten myöntämisestä vastaavien jäsenvaltioiden yksiköiden pääsyn sallimisesta toisen sukupolven Schengenin tietojärjestelmään (SIS II) (KOM (2005) 237 lopullinen)

(2006/C 91/11)

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 17 päivänä kesäkuuta 2005 komissiolta saadun, asetuksen (EY) N:o 45/2001 28 artiklan 2 kohdan mukaisen lausuntopyynnön,

ON ANTANUT SEURAAVAN LAUSUNNON:

1. JOHDANTO

1.1 Taustaa

Schengenin tietojärjestelmä (SIS) on EU:n laaja tietotekninen järjestelmä, joka luotiin kompensoivaksi järjestelmäksi, kun tarkastukset Schengen-alueen sisärajoilla lopetettiin. SIS:n avulla jäsenvaltioiden toimivaltaiset viranomaiset voivat vaihtaa tietoja, joita käytetään jäsenvaltioiden ulkorajoilla tai alueilla tehtävissä henkilöiden ja tavaroiden tarkastuksissa sekä viisumien ja oleskelulupien myöntämisessä.

Schengenin yleissopimus tuli voimaan 1995 hallitusten välisenä sopimuksena. SIS, joka on osa Schengenin yleissopimusta, sisällytettiin myöhemmin Amsterdamin sopimuksella osaksi EU:n säädöspuitteita.

Uusi, ns. toisen sukupolven Schengenin tietojärjestelmä II korvaa nykyisen järjestelmän, ja näin myös EU:n uudet jäsenvaltiot voidaan liittää Schengen-alueeseen. Uudessa järjestelmässä on myös joitain uusia toimintoja. Schengenin säännöstö, joka laadittiin hallitusten välisenä yhteistyönä, muunnetaan kokonaisuudessaan perinteiseksi EU:n lainsäädännöksi.

Euroopan komissio antoi 1.6.2005 kolme ehdotusta SIS II -järjestelmän perustamiseksi. Nämä kolme ehdotusta ovat:

— asetusehdotus, joka perustuu EY:n perustamissopimuksen IV osastoon (viisumiasiat, turvapaikka- ja maahanmuuttoasiat ja muut henkilöiden vapaaseen liikkuvuuteen liittyvät politiikat) ja joka kattaa ensimmäisen pilarin (maahanmuutto) näkökohdat SIS II -järjestelmässä, jäljempänä 'asetusehdotus';

— päätösehdotus, joka perustuu SEU:n VI osastoon (poliisi- ja oikeudellinen yhteistyö rikosasioissa) ja joka kattaa SIS:n käytön kolmanteen pilariin kuuluvissa asioissa, jäljempänä 'päätösehdotus';

— asetusehdotus, joka perustuu V osastoon (liikenne) ja joka koskee erityisesti ajoneuvojen rekisteröimisestä vastaavien viranomaisten oikeutta käyttää SIS:n tietoja; tätä ehdotusta käsitellään erikseen (ks. kohta 4.6).

Tässä yhteydessä on syytä mainita, että komissio antaa lähikuukausina tiedonannon EU:n tietojärjestelmien (SIS, VIS, Eurodac) yhteentoimivuudesta ja niiden välisestä lisääntyneestä synergiasta.

SIS II koostuu keskustietokannasta, jäljempänä 'Schengenin keskustietojärjestelmä' (CS-SIS), jonka operatiivisesta hallinnoinnista komissio vastaa; keskustietokanta on liitetty kunkin jäsenvaltion määrittämiin kansallisiin liityntäpisteisiin (NI-SIS). SIRENE-viranomaiset huolehtivat kaikkien lisätietojen vaihdosta (SIS II -järjestelmän ilmoituksiin liittyvät tiedot, joita ei tallenneta SIS II -järjestelmään).

Jäsenvaltiot syöttävät SIS II -järjestelmään tietoja henkilöistä, joita etsitään pidätystä, luovuttamista tai rikoksen johdosta tapahtuvaa luovuttamista varten taikka oikeuskäsittelyjä varten, tarkkailuun asetettavista henkilöistä tai henkilöistä, joille on määrä tehdä erityistarkastuksia tai joilta evätään maahanpääsy ulkorajoilla, sekä kadonneista tai varastetuista esineistä. SIS-järjestelmään vietyjen ns. ilmoitusten avulla toimivaltaiset viranomaiset voivat tunnistaa henkilön tai esineen.

SIS II -järjestelmässä on uusia piirteitä: järjestelmän käyttöoikeuksia on laajennettu (Europol, Eurojust, jäsenvaltioiden yleiset syyttäjät, ajoneuvojen rekisteröinnistä vastaavat viranomaiset), ilmoitukset on linkitetty, uusia tietoluokkia on lisätty, mukaan lukien biometriset tiedot (sormenjäljet, valokuvat), ja samaa teknistä alustaa voidaan nyt käyttää myös viisumitietojärjestelmässä (VIS). Näistä lisäpiirteistä on keskusteltu vuosien ajan, koska ne on nähty SIS:n tarkoituksen muuttumisena niin, että valvontavälineestä tulee raportointi- ja tutkintaväline.

1.2 **Yleinen arvio ehdotuksista**

1. Euroopan tietosuojavaltuutettu on tyytyväinen siihen, että häntä kuullaan asetuksen (EY) N:o 45/2001 28 artiklan perusteella. Koska tämä kuuleminen on kyseisen 28 artiklan 2 kohdan mukaan pakollista, tämä lausunto olisi mainittava säädösten johdanto-osassa.

2. Euroopan tietosuojavaltuutettu suhtautuu ehdotuksiin myönteisesti useasta syystä. Hallitusten välisen rakenteen muuttamisella Euroopan lainsäädäntövälineiksi on useita myönteisiä seurauksia: SIS II -järjestelmää koskevien sääntöjen oikeudellinen merkitys selkiytyy, yhteisöjen tuomioistuimella on toimivalta tulkita ensimmäisen pilarin alaan kuuluvia säädöksiä, Euroopan parlamentti voi osallistua ainakin osittain asian käsittelyyn (vaikkakin melko myöhäisessä vaiheessa prosessia).

3. Ehdotukset sisältävät lisäksi huomattavan määrän tietosuojaan liittyviä kohtia, joista jotkin ovat tervetulleita parannuksia nykytilanteeseen. Erityisesti voidaan mainita seuraavaa: toimenpiteet henkilöllisyyden väärinkäytön kohteeksi joutuneiden henkilöiden hyväksi, asetuksen (EY) N:o 45/2001 laajentaminen VI osastoon kuuluviin komission suorittamiin tietojen käsittelytoimiin, paremmat perustelut sille, että henkilöistä on tehty järjestelmään ilmoitus maahanpääsyn epäämiseksi.

4. On myös ilmeistä, että ehdotukset on laadittu huolellisesti; ne ovat mutkikkaita, mutta tämä kuvastaa niiden kattaman järjestelmän mutkikkuutta. Suurin osa tässä lausunnossa esitetyistä kommenteista on tarkoitettu selkeyttämään tai täydentämään säännöksiä, mutta kokonaan uusien ehdotusten laatimista ei niissä edellytetä.

Vaikka kokonaisarvio onkin myönteinen, voidaan esittää joitakin varaumia erityisesti seuraavista seikoista:

1. Monesti on vaikea tietää, mitä tekstillä tarkoitetaan. Selitysosan puuttuminen on hyvin valitettavaa. Näiden asiakirjojen mutkikkuuden vuoksi selitysosan olisi pitänyt kuulua niihin perusvaatimuksena. Sen puuttumisen vuoksi lukijan on joskus tyydyttävä arvauksiin.

2. Valitettavaa on myös vaikutustenarvioinnin puuttuminen. Tämä ei ole perusteltavissa sillä, että järjestelmän ensimmäinen versio on jo käytössä, sillä ensimmäisen ja uuden version välillä on huomattavia eroja. Esimerkiksi biometristen tietojen sisällyttämisen vaikutuksia olisi pitänyt pohtia tarkemmin.

3. Tietosuojaa koskeva oikeussäännöstö on hyvin monimutkainen: siihen sovelletaan yhtä aikaa yleissääntöä (*lex generalis*) ja erityissääntöä (*lex specialis*). Olisi huolehdittava siitä, että vaikka kehitetään erityislainsäädäntöä, direktiivin 95/46/EY ja asetuksen 45/2001 nykyistä tietosuojasäännöstöä on sovellettava täysin. Eri lainsäädäntövälineiden yhdisteleminen ei saisi johtaa siihen, että kansallisten järjestelmien välille syntyy ristiriita perusnäkökohtien osalta. Toisaalta nykyistä tietosuojatasoa ei myöskään tulisi madaltaa.

4. Koska useat uudet viranomaiset, jotka eivät kuulu alkuperäiseen "henkilöiden ja esineiden valvonta" -kategoriaan, saavat oikeuden käyttää järjestelmää, tulisi suojatoimia tiukentaa.

5. Ehdotukset perustuvat suurelta osin muihin lainsäädäntövälineisiin, joita ollaan vielä valmistelemassa (tai joita ei ole vielä edes ehdotettu). Euroopan tietosuojavaltuutettu ymmärtää, mitä vaikeuksia lainsäädäntötyöhön mutkikkaassa ja jatkuvasti muuttuvassa ympäristössä liittyy, mutta ottaen huomioon seuraukset niille henkilöille, joita asia koskee, ja tästä aiheutuvan oikeudellisen epävarmuuden, se ei pidä tätä hyväksyttävänä.

6. Jäsenvaltioiden ja komission välisessä toimivaltajaossa on epäselvyyttä. Selkeys on ensiarvoisen tärkeää paitsi järjestelmän toimivuuden kannalta myös siksi, että se on perusedellytys järjestelmän kattavan valvonnan varmistamiseksi.

1.3 **Lausunnon rakenne**

Tämän lausunnon rakenne on seuraavanlainen: siinä selvitetään ensin SIS II -järjestelmään sovellettavaa oikeudellista kehystä. Sen jälkeen käsitellään SIS II -järjestelmän tarkoituksen määritelmää ja nykyjärjestelmästä huomattavasti poikkeavia osia. Kohdassa 5 on huomioita komission ja jäsenvaltioiden tehtävistä SIS II -järjestelmän toiminnan kannalta. Kohdassa 6 käsitellään niiden rekisteröityjen oikeuksia ja kohdassa 7 valvontaa jäsenvaltioiden tasolla ja Euroopan tietosuojavaltuutetun suorittamana sekä valvojien yhteistyötä. Kohdassa 8 on huomioita turvallisuudesta ja siinä ehdotetaan mahdollisia tarkistuksia. Kohdissa 9 ja 10 käsitellään komiteamenettelyä ja yhteentoimivuutta. Lopuksi yhteenvedossa tuodaan esiin kunkin kohdan pääasialliset huomiot.

2. ASIAA KOSKEVA LAINSÄÄDÄNTÖKEHYS

2.1 **SIS II -järjestelmää koskeva tietosuojasäännöstö**

Ehdotuksissa viitataan niiden tietosuojaa koskevina lainsäädäntökehyksinä direktiiviin 95/46/EY, yleissopimukseen N:o 108 ja asetukseen 45/2001. Myös muut välineet ovat tässä merkityksellisiä.

Tämän asian selventämiseksi ja muistuttaaksemme siitä, mitkä tarkastelumme lähtökohdat ovat, on syytä esittää seuraavat seikat:

— Oikeus nauttia yksityiselämän kunnioitusta on varmistettu Euroopassa vuodesta 1950 lähtien, jolloin Euroopan neuvosto hyväksyi ihmisoikeuksien ja perusvapauksien suojaamista koskevan yleissopimuksen (jäljempänä 'ECHR'). Kyseisen yleissopimuksen 8 artiklassa määrätään oikeudesta nauttia yksityis- ja perhe-elämän kunnioitusta.

  Kyseisen yleissopimuksen 8 artiklan 2 kohdan mukaan "viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä" tärkeiden etujen suojelemiseksi. Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä nämä ehdot ovat johtaneet lisävaatimuksiin oikeuksiin puuttumisen oikeusperustan, toimenpiteiden suhteellisuuden ja väärinkäytöksiltä suojaamisen osalta.

— Oikeus nauttia yksityiselämän kunnioitusta ja oikeus henkilötietojen suojeluun on sittemmin sisällytetty Euroopan unionin perusoikeuskirjan 7 ja 8 artiklaan. Perusoikeuskirjan 52 artiklan mukaan näitä oikeuksia voidaan rajoittaa edellyttäen, että ECHR:n 8 artiklan mukaisia ehtoja noudatetaan.

— Euroopan unionista tehdyn sopimuksen 6 artiklan 2 kohdassa määrätään, että unioni noudattaa ECHR:n mukaisia perusoikeuksia.

Kolme nimenomaisesti SIS II -järjestelmää koskeviin ehdotuksiin sovellettavaa tekstiä ovat seuraavat:

— Euroopan neuvoston yleissopimus N:o 108 yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (jäljempänä 'yleissopimus N:o 108'; tehty 28.1.1981), jossa annetaan perusperiaatteet yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä. Kaikki jäsenvaltiot ovat ratifioineet kyseisen yleissopimuksen, ja sitä sovelletaan myös poliisi- ja oikeudellisen alan toimiin. Yleissopimus N:o 108 on tällä hetkellä SIS-yleissopimukseen sovellettava tietosuojajärjestelmä yhdessä Euroopan neuvoston ministerikomitean antaman suosituksen N:o R (87) 15 kanssa (annettu 17.9.1987), joka säätelee tietojen käyttöä poliisialalla.

— Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (annettu 24.10.1995; EYVL L 281, s. 31), jäljempänä *'direktiivi 95/46/EY'*. On huomattava, että useimmissa jäsenvaltioissa direktiivin täytäntöönpanemiseksi annettu lainsäädäntö kattaa myös poliisi- ja oikeudellisella alalla tapahtuvan tietojen käsittelyn.

— Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (annettu 18.12.2000; EYVL L 8, s. 1), jäljempänä *'asetus 45/2001"*.

Direktiivin 95/46/EY ja asetuksen 45/2001 tulkinnassa on otettava huomioon myös ihmisoikeuksien ja perusvapauksien suojaamisesta tehdyn vuoden 1950 yleissopimuksen (ECHR) mukainen, Euroopan ihmisoikeustuomioistuimen asiaa koskeva oikeuskäytäntö. Toisin sanoen direktiiviä ja asetusta on tulkittava perusoikeuksien valossa, jos niissä puututaan henkilötietojen käsittelyyn, joka saattaisi loukata perusvapauksia, erityisesti yksityisyyden suojaa koskevaa oikeutta. Tämä on myös Euroopan yhteisöjen tuomioistuimen oikeuskäytännön mukaista. [1]

[1] Tässä yhteydessä on syytä viitata tuomioistuimen tuomioon asiassa Österreichischer Rundfunk ym. (yhdistetyt asiat C-465/00, C-138/01 ja C-139/01), tuomio 20.5.2003, tuomioistuimen täysistunto, (2003) Kok. I-4989. Tuomioistuin käsitteli Itävallan lakia, jonka mukaan julkisen sektorin palveluksessa olevien henkilöiden tulot on ilmoitettava Itävallan Rechnungshofille ja lisäksi julkistettava. Tuomiossaan tuomioistuin esittää joukon perusteita, jotka perustuvat ECHR:n 8 artiklaan ja joita tulisi käyttää sovellettaessa direktiiviä 95/46/EY siltä osin kuin tämä direktiivi antaa mahdollisuuden tiettyihin rajoituksiin, jotka koskevat oikeutta yksityisyyteen.

Komissio antoi 4.10.2005 ehdotuksen neuvoston puitepäätökseksi rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta ([1]) (jäljempänä *'ehdotus puitepäätökseksi'*). Tällä puitepäätöksellä on tarkoitus korvata yleissopimus N:o 108 SIS II -järjestelmää koskevan päätösehdotuksen lainsäädäntöviitteenä, mikä vaikuttaa todennäköisesti tietosuojajärjestelmään (ks. kohta 2.2.5).

2.2 **SIS II -järjestelmää säätelevä tietosuojajärjestelmä**

2.2.1 *Yleisiä huomioita*

SIS II -järjestelmän edellyttämä oikeusperusta koostuu erillisistä säädöksistä, mutta kuten johdanto-osissa todetaan, "SIS II muodostaa yhden ainoan tietojärjestelmän, jonka olisi toimittava sellaisena. Sen vuoksi näiden säädösten tiettyjen säännösten olisi oltava samanlaiset."

Näiden kahden asiakirjan rakenne on perusteeltaan sama, ja luvut I–III ovat lähes identtiset kummassakin tekstissä. Se, että SIS II -järjestelmää on pidettävä yhtenä ainoana tietojärjestelmänä, jolla on kaksi eri oikeusperustaa, näkyy myös melko mutkikkaassa tietosuojajärjestelmässä.

Tietosuojajärjestelmä on määritelty osittain jo itse ehdotuksissa (ns. *lex specialis*), ja sitä on täydennetty kunkin alan (komissio, jäsenvaltiot ensimmäisen pilarin osalta, jäsenvaltiot kolmannen pilarin osalta) viitelainsäädännöllä (ns. *lex generalis*).

Tämä rakenne herättää kysymyksen siitä, miten erityissääntöjen kanssa menetellään suhteessa yleiseen lainsäädäntöön. Euroopan tietosuojavaltuutettu katsoo tässä tapauksessa erityissäännön olevan yleisen säännön soveltamista. Näin ollen erityissäännön (*lex specialis*) on aina oltava yhdenmukainen yleissäännön (*lex generalis*) kanssa: se kehittää (täsmentää tai täydentää) yleissääntöä mutta ei muodosta siihen poikkeusta.

Sen suhteen, mitä sääntöä olisi sovellettava erityistapauksissa, periaatteena on, että erityissääntöä sovelletaan ensisijaisesti. Jos se ei anna vastausta tai on epäselvä, on otettava huomioon yleissääntö.

Tämän rakenteen huomioon ottaen on olemassa kolme erilaista yleissäännön ja erityissäännön yhdistelmää. Seuraavassa esitetään asiasta yhteenveto.

2.2.2 *Komissiossa sovellettava järjestelmä*

Kun komissiosta on kyse, sovelletaan asetusta 45/2001, mukaan lukien Euroopan tietosuojavaltuutetun rooli, olivatpa toimet ensimmäiseen (asetusehdotus) tai kolmanteen pilariin (päätösehdotus) kuuluvia. Päätösehdotuksen johdanto-osan 21 kappaleessa todetaan: "(…) asetusta (EY) N:o 45/2001 sovelletaan komission suorittamaan henkilötietojen käsittelyyn, kun se liittyy toimintoihin, joista ainakin osa kuuluu yhteisön lainsäädännön soveltamisalaan. Osa henkilötietojen käsittelystä SIS II -järjestelmässä kuuluu yhteisön lainsäädännön soveltamisalaan".

Tälle on olemassa käytännön syyt: komission tapauksessa olisi erittäin vaikeaa määritellä, käsitelläänkö tietoja ensimmäisen vai kolmannen pilarin alaan kuuluvien toimien yhteydessä.

Lisäksi yhden ainoan oikeudellisen välineen soveltaminen kaikkiin komission toimiin SIS II:n yhteydessä on käytännön kannalta paitsi järkevää myös parantaa johdonmukaisuutta (varmistaa asetusehdotuksen johdanto-osan 21 kappaleen mukaan "Yksilöiden perusoikeuksien ja -vapauksien suojelua henkilötietojen käsittelyssä koskevien sääntöjen johdonmukaisen ja yhtenäisen soveltamisen"). Tästä syystä Euroopan tietosuojavaltuutettu on tyytyväinen komission toteamukseen, että asetusta 45/2001 sovelletaan kaikkeen tietojen käsittelyyn, jota komissio suorittaa SIS II -järjestelmässä.

2.2.3 *Jäsenvaltioissa sovellettava järjestelmä*

Jäsenvaltioiden tilanne on mutkikkaampi. Henkilötietojen käsittelyä asetusehdotuksessa esitetyn mukaisesti säätelevät asetusehdotuksen säännökset ja direktiivin 95/46/EY säännökset. Asetusehdotuksen johdanto-osan 14 kappaleesta käy selvästi ilmi, että direktiiviä on pidettävä yleissääntönä (*lex generalis*), ja SIS II -asetusta erityissääntönä (*lex specialis*). Tällä on joitakin seurauksia, joita käsittelemme jäljempänä.

Päätösehdotuksen osalta taas tietosuojaa koskeva oikeudellinen väline, johon viitataan (*lex generalis*), on yleissopimus N:o 108, mikä saattaa aiheuttaa huomattavia eroja ensimmäisen ja kolmannen pilarin tietosuojajärjestelmissä joiltain osin.

2.2.4 *Vaikutus tietosuojan tasoon*

Tietosuojajärjestelmää koskevana yleisenä kommenttina Euroopan tietosuojavaltuutettu toteaa seuraavaa:

— Ehdotetun asetuksen soveltaminen direktiivin 95/46/EY erityissääntönä *(lex specialis)* ja samoin ehdotetun päätöksen soveltaminen yleissopimuksen N:o 108 erityissääntönä ei saisi johtaa direktiivin tai yleissopimuksen mukaisen tietosuojatason alenemiseen. Euroopan tietosuojavaltuutettu antaa asiasta suosituksia (ks. esimerkiksi kanneoikeus).

([1]) KOM (2005) 475 lopull.

— Säädösten yhdistetty käyttö ei myöskään saa johtaa siihen, että nykyinen Schengenin yleissopimuksen mukainen tietosuojataso alenee (ks. esimerkiksi direktiivin 95/46/EY 13 artiklasta jäljempänä esitetyt huomautukset).

— Olipa kahden erilaisen välineen soveltaminen kuinka tärkeää tahansa Eurooppa-oikeuden kannalta, se ei saisi johtaa perusteettomiin ristiriitaisuuksiin asianomaisten henkilöiden tietosuojan välillä sen mukaan, mitä heidän tietojaan käsitellään. Tätä on vältettävä niin pitkälle kuin mahdollista. Jäljempänä esitetyillä suosituksilla pyritään myös parantamaan johdonmukaisuutta mahdollisimman paljon (ks. esimerkiksi kansallisten valvontaviranomaisten toimivalta).

— Oikeudelliset puitteet ovat niin monimutkaiset, että se todennäköisesti aiheuttaa hämmennystä käytännössä. Joissain tapauksissa on vaikea nähdä, miten *lex generalis* ja *lex specialis* toimivat yhdessä, ja tätä olisikin hyvä selventää ehdotuksissa. Lisäksi tässä mutkikkaassa lainsäädäntöympäristössä Schengenin yhteisen valvontaviranomaisen SIS II:n ehdotetusta oikeusperustasta antamassa lausunnossa (27.9.2005) esitetty ehdotus ”käsikirjasta”, jossa lueteltaisiin kaikki nykyiset SIS II -järjestelmään liittyvät oikeudet ja esitettäisiin selkeä hierarkia sovellettavasta lainsäädännöstä, on hyvin hyödyllinen.

Tässä lausunnossa pyritään varmistamaan korkea tietosuojan taso, johdonmukaisuus ja selkeys, jotta henkilöllä, jonka tietoja käsitellään, on tarvittava oikeusvarmuus.

2.2.5 *Puitepäätösehdotuksen vaikutus kolmannen pilarin alaan kuuluvaan tietosuojaan*

Yleissopimus N:o 108 SIS II -järjestelmää koskevan päätösehdotuksen tietosuojasäädöksenä korvataan kolmannen pilarin alaan kuuluvaa tietosuojaa koskevalla puitepäätöksellä. ([1]) Tätä ei mainita ehdotuksessa, mutta se on seurausta ehdotetusta puitepäätöksestä. Sen 34 artiklan 2 kohdassa todetaan, että kaikki viittaukset 28.1.1981 tehtyyn Euroopan neuvoston yleissopimukseen N:o 108 yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä on ymmärrettävä viittauksiksi tähän puitepäätökseen. Euroopan tietosuojavaltuutettu antaa lähiviikkoina lausunnon puitepäätösehdotuksesta eikä näin ollen analysoi sen sisältöä tässä lausunnossa. Aina kun puitepäätöksen soveltaminen voi vaikuttaa huomattavasti SIS II:n tietosuojajärjestelmään, tämä mainitaan.

2.2.6 *Direktiivin 95/46/EY 13 artiklan ja yleissopimuksen N:o 108 9 artiklan soveltaminen*

Direktiivin 95/46/EY 13 artiklassa ja yleissopimuksen N:o 108 9 artiklassa säädetään, että jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan säädettyjen oikeuksien ja velvoitteiden alaa, jos tällaiset rajoitukset ovat välttämättömiä muiden tärkeiden etujen suojaamiseksi (esim. valtion turvallisuus, puolustus, yleinen turvallisuus) ([2]).

Sekä asetusehdotuksen että päätösehdotuksen johdanto-osan kappaleissa mainitaan, että jäsenvaltio voi käyttää tätä mahdollisuutta pannessaan ehdotuksia täytäntöön kansallisesti. Tällöin olisi todennettava, että direktiivin 95/46/EY 13 artiklan soveltaminen ei ole ristiriidassa ECHR:n 8 artiklan kanssa ja että se ei johda nykyisen tietosuojajärjestelmän heikkenemiseen.

Tämä on erityisen tärkeää SIS II:n kohdalla, sillä järjestelmän on oltava ennakoitavissa. Koska jäsenvaltiot jakavat tietoja, on voitava tietää kohtalaisella varmuudella, miten tietoja käsitellään kansallisesti.

Tähän liittyy erityisesti yksi huolestuttava puoli. Ehdotukset saattaisivat johtaa nykyisen tietosuojatason alenemiseen. Schengenin yleissopimuksen 102 artiklassa määrätään järjestelmästä, jossa tietojen käyttö on tiukasti säädeltyä ja rajoitettua, jopa kansallisessa lainsäädännössä (”Edellä olevan 1–4 kappaleen vastaista tietojenkäyttöä pidetään väärinkäyttönä kunkin sopimuspuolen kansallisen lainsäädännön mukaisesti.”) Sekä direktiivissä 95/46/EY että yleissopimuksessa N:o 108 säädetään kuitenkin, että poikkeuksia muun muassa tarkoituksen rajoittamista koskevaan periaatteeseen voidaan ottaa käyttöön kansallisessa lainsäädännössä. Jos näin tapahtuu, se olisi ristiriidassa Schengenin yleissopimuksen nykyisen järjestelmän kanssa, jossa kansallinen lainsäädäntö ei voi poiketa käyttötarkoituksen ja käytön rajoittamista koskevasta perusperiaatteesta.

Puitepäätöksen hyväksyminen ei muuttaisi tätä huomiota: ongelma on pikemminkin se, että tiukka käyttötarkoituksen rajoittamisen periaate säilytetään SIS II:n tietojen käsittelyssä, kuin että varmistetaan tietojen käsittely puitepäätöksen mukaisesti.

([1]) Se korvaa myös Schengenin yleissopimuksen yleisen tietosuojajärjestelmän (Schengenin yleissopimuksen 126—130 artikla). Tätä järjestelmää ei sovelleta SIS:ään.

([2]) Jäsenvaltio, joka haluaa käyttää tätä mahdollisuutta oikeuksien rajoittamiseen, voi tehdä näin vain noudattamalla ECHR:n 8 artiklaa, kuten edellä todettiin.

Euroopan tietosuojavaltuutettu ehdottaa, että SIS II -ehdotuksiin (asetusehdotuksen 21 artiklaan ja päätösehdotuksen 40 artiklaan) lisätään samantyyppinen säännös kuin Schengenin yleissopimuksen 102 artiklan 4 kohdassa, jossa rajoitetaan jäsenvaltioiden mahdollisuutta säätää tietojen käytöstä, josta ei ole mainintaa SIS II:sta koskevissa teksteissä. Toinen mahdollisuus on rajoittaa päätösehdotuksessa ja asetusehdotuksessa nimenomaisesti niiden poikkeusten soveltamisalaa, joita voidaan käyttää direktiivin 13 artiklan tai yleissopimuksen 9 artiklan nojalla. Voidaan säätää esimerkiksi siitä, että jäsenvaltiot voivat asettaa rajoituksia vain käyttöoikeuksille ja tiedonsaannille, mutta eivät tietojen laadun periaatteille.

3. **TARKOITUS**

Kyseessä olevan kahden asiakirjan 1 artiklan (”SIS:n perustaminen ja yleiset tavoitteet”) mukaan SIS II perustetaan, jotta ”jäsenvaltioiden toimivaltaiset viranomaiset voivat tehdä yhteistyötä vaihtamalla tietoja henkilöitä ja esineitä koskevia tarkastuksia varten” ja se ”auttaa säilyttämään korkean turvallisuuden tason alueella, jonka sisärajoilla ei tehdä tarkastuksia”.

SIS II:n tarkoitus on muotoiltu melko laveasti; edellä mainitut säännökset eivät itsessään täsmennä, mitä tähän tavoitteeseen sisältyy (ja mitä sillä tarkoitetaan).

SIS II:n tavoite näyttää paljon laajemmalta kuin nykyisen SIS:n tavoite, sellaisena kuin se on määritelty Schengenin yleissopimuksen 92 artiklassa, jossa todetaan erityisesti, että ”(Schengenin tietojärjestelmän kautta sopimuspuolten nimeämät viranomaiset pääsevät …) käsiksi henkilöistä ja tavaroista tehtyihin ilmoituksiin rajatarkastusten ja -valvonnan yhteydessä ja muiden (…) poliisi- ja tullitarkastusten yhteydessä sekä (96 artiklassa tarkoitettujen ilmoitusten osalta) viisumien ja oleskelulupien myöntämistä ja ulkomaalaishallintoa varten (…)”.

Tämä laajempi tarkoitus johtuu myös siitä, että SIS II -järjestelmään on lisätty uusia toimintoja ja käyttöoikeuksia, jotka eivät ole alkuperäisen tarkoituksen (henkilöiden ja tavaroiden tarkastukset) mukaisia, vaan pikemminkin tutkimusvälineen käyttötarkoituksen mukaisia. Käyttöoikeus annetaan erityisesti viranomaisille, jotka käyttävät SIS II:n tietoja omiin tarkoituksiinsa, eikä SIS II:n tarkoitusten toteuttamiseksi (ks. alla); ilmoitusten linkittäminen keskenään yleistyy, sillä tämä on tyypillistä poliisin tutkintavälineille.

On myös virinnyt kysymyksiä biometrisestä hakukoneesta, joka on määrä kehittää tulevina vuosina ja jonka avulla järjestelmässä voidaan tehdä hakuja, jotka ylittävät valvontajärjestelmän tarpeet.

Ehdotuksilla on siis paljon laajempi soveltamisala kuin nykyisillä säädöksillä. Tämä edellyttää lisäturvatoimia. Euroopan tietosuojavaltuutettu ei keskitä analyysiään 1 artiklan laajaan määrittelyyn sellaisenaan, vaan SIS II:n toimintoihin ja muihin rakenteellisiin osiin.

4. **HUOMATTAVAT MUUTOKSET SIS II:SSA**

Tässä luvussa keskitytään ensiksi SIS II:n uusiin osiin, erityisesti biometriikan sisällyttämiseen, uusiin, eritoten Europolille ja Eurojustille annettaviin käyttöoikeuksiin, ajoneuvojen rekisteröinnistä vastaavien viranomaisten käyttöoikeuksiin, ilmoitusten linkitykseen ja eri viranomaisten mahdollisuuteen saada oikeus käyttää maahanmuuttotietoja.

4.1. **Biometriikka**

SIS II:sta koskevissa ehdotuksissa otetaan käyttöön mahdollisuus käsitellä uutta tietoluokkaa, johon on syytä kiinnittää erityistä huomiota. Kuten Euroopan tietosuojavaltuutettu toteaa viisumitietojärjestelmää koskevassa lausunnossaan ([1]), biometrisille tiedoille ominainen arkaluonteisuus edellyttää erityisiä suojatoimia, joita ei ole sisällytetty SIS II:sta koskeviin ehdotuksiin.

Yleisenä huomiona voidaan todeta, että biometristen tietojen käyttäminen EU:n laajuisissa tietojärjestelmissä (VIS, Eurodac, ajokortteja koskeva tietojärjestelmä jne.) yleistyy koko ajan, mutta samanaikaisesti ei kuitenkaan ole huolellisesti harkittu siihen liittyviä riskejä ja tarvittavia suojatoimia.

Tämä syvällisemmän pohdinnan tarve on otettu esiin myös Montreux’ssä kokoontuneiden tietosuojavaltuutettujen kansainvälisessä konferenssissa äskettäin annetussa biometriikkaa koskevassa päätöslauselmassa ([2]). Tähän saakka standardien kehittämisestä saatava lisäarvo on suunnattu järjestelmien väliseen yhteentoimivuuteen eikä biometristen menettelyjen laadun parantamiseen.

([1]) Euroopan tietosuojavaltuutetun lausunto ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta, 23.3.2005, kohta 3.4.2.

([2]) 27. kansainvälinen tietosuojavaltuutettujen konferenssi, Montreux, 16.9.2005, Päätöslauselma biometriikan käytöstä passeissa, henkilötodistuksissa ja matkustusasiakirjoissa.

Olisi hyvä laatia yhteiset velvoitteet tai vaatimukset, jotka liittyvät tällaisten tietojen erityislaatuun, sekä yhteinen menetelmä niiden täytäntöönpanemiseksi. Näihin yhteisiin vaatimuksiin voisi sisältyä erityisesti seuraavaa (näiden seikkojen tarve näkyy SIS II:sta koskevissa ehdotuksissa):

— **Kohdennettu vaikutustenarviointi**: On syytä korostaa, että ehdotuksiin sisältyvästä biometriikan käytöstä ei ole tehty vaikutustenarviointia ([1]).

— **Rekisteröintimenettelyn korostaminen**: Biometristen tietojen lähdettä ja tapaa, jolla tiedot kerätään, ei ole määritelty yksityiskohtaisesti. Rekisteröinti on yksi biometrisen tunnistusmenettelyn kriittisistä vaiheista eikä sitä voida määritellä pelkästään liitteissä tai alatyöryhmäkeskusteluissa, koska se vaikuttaa suoraan menettelyn lopputulokseen eli siihen, miten suuri väärin perustein tapahtuvan hylkäämisen/hyväksymisen aste (False Rejection rate/False Acceptance rate) on.

— **Tarkkuuden painottaminen**: Biometriikan käyttö tunnistamiseen (yhden vertaaminen moniin), mikä ehdotuksen mukaisesti toteutuisi tulevaisuudessa "biometrisena hakukoneena", on arveluttavampaa, koska tällaisen menettelyn tulokset eivät ole yhtä tarkkoja kuin käytettäessä biometriikkaa varmistamiseen tai valvontaan (yhden vertaaminen yhteen). Biometrisen tunnistamisen ei pitäisikään olla ainoa tunnistamiskeino tai ainoa tapa saada lisätietoja.

— **Varamenettely:** Jo saatavilla olevia varamenettelyjä on otettava käyttöön sellaisten henkilöiden suojelemiseksi, jotka on saatettu tunnistaa virheellisesti ja sen estämiseksi, että he joutuisivat kärsimään järjestelmän vioista.

Biometristen tietojen käyttö ilman asianmukaista ennakkoarviointia on myös osoitus biometriikan luotettavuuden yliarvioinnista. Biometriset tiedot ovat elävää ja ajan myötä muuttuvaa tietoa. Tietokantaan tallennetut näytteet ovat vain otteita dynaamisesta elementistä tietyllä hetkellä. Niiden pysyvyys ei ole ehdotonta ja niitä on siten valvottava. Biometriikan tarkkuus on aina suhteutettava muihin tekijöihin, sillä se ei koskaan ole ehdoton.

([1]) Arviointi voisi perustua biometrisen tiedon ns. seitsemään pilariin, ks. "Biometrics at the frontiers: Assessing the impact on Society" IPTS, DG-JRC, EUR 21585 EN, osa 1.2, s. 32.

SIS II:n tietojen mahdollinen käyttö tutkintatarkoituksiin sisältää vakavia riskejä henkilölle, jota tiedot koskevat, jos biometristen todisteiden merkitystä korostetaan tai yliarvioidaan, kuten aiemmin on käynyt ilmi ([2]).

Ehdotuksissa olisi näin ollen tunnustettava ja tiedostettava biometriikan todellinen käyttöarvo tunnistamistarkoituksissa.

4.2 **SIS II -tietojen käyttöoikeus**

4.2.1 *Uudenlainen käyttöoikeus*

Viranomaiset, jotka voivat käyttää SIS-tietoja, määritellään jokaisen ilmoituksen osalta erikseen. Periaatteessa oikeus käyttää SIS-tietoja annetaan soveltaen kahta perustetta: viranomaisille annettavan käyttöoikeuden on oltava täysin SIS:n yleisen tarkoituksen ja kunkin ilmoituksen erityistarkoituksen mukainen.

Tämä johtuu sekä asetus- että päätösehdotuksessa olevista ilmoitusten määritelmistä (kummankin säädöksen 3 artiklan 1 kohdan a alakohdan mukaan "*'ilmoituksella' tarkoitetaan SIS II -järjestelmään tallennettuja tietoja, joiden avulla toimivaltaiset viranomaiset voivat tunnistaa henkilön tai esineen tietyn toimenpiteen toteuttamiseksi*"). Kyseistä näkemystä vahvistaa päätösehdotuksen 39 artiklan 2 kohta, jonka mukaan "*edellä 1 kohdassa tarkoitettuja tietoja voidaan käyttää ainoastaan henkilön tunnistamiseen tietyn toimenpiteen toteuttamiseksi tämän päätöksen mukaisesti*." Tässä suhteessa SIS II -järjestelmässä on vielä piirteitä osuma/ei osumaa -järjestelmästä, jossa jokainen ilmoitus tallennetaan tiettyä tarkoitusta varten (mm. luovutus, maahanpääsyn epääminen).

Viranomaisilla, joilla on oikeus saada SIS-tietoja, on todellisuudessa rajoitettu käyttöoikeus kyseisiin tietoihin, koska ne voivat periaatteessa saada ainoastaan tietyn toimenpiteen toteuttamiseen tarvittavia tietoja.

Jotkut uusiin ehdotuksiin sisältyvät käyttöoikeudet eivät kuitenkaan ole johdonmukaisia kyseisen logiikan kanssa: niiden tarkoituksena on itse asiassa antaa viranomaisille tietoja antamatta kuitenkaan mahdollisuutta tunnistaa henkilö tai toteuttaa ilmoituksen mukaisia toimenpiteitä.

([2]) Kesäkuussa 2004 Portlandista (USA) kotoisin oleva lakimies joutui kahdeksi viikoksi vankilaan, koska FBI oli onnistunut täsmäämään hänen sormenjälkensä Madridin pommi-iskussa (sytyttimen sisältäneestä muovikassista) löytyneisiin sormenjälkiin. Lopulta saatiin osoitettua, että vertailumenettely oli puutteellinen, mikä johti väärään tulkintaan.

Tämä koskee erityisesti:

— turvapaikkaviranomaisten oikeutta käyttää maahanmuuttotietoja;

— pakolaisaseman myöntämisestä vastaavien viranomaisten oikeutta käyttää maahanmuuttotietoja;

— Europolin oikeutta käyttää ilmoituksia, jotka koskevat rikoksen johdosta luovuttamista, tarkkailua ja varastettuja asiakirjoja takavarikointia varten;

— Eurojustin oikeutta käyttää rikoksen johdosta luovuttamista ja paikantamista koskevia tietoja.

SIS II -tietojen osalta kaikilla kyseisillä viranomaisilla on samat ominaisuudet:

ne eivät voi toteuttaa ilmoitusten määritelmässä mainittuja tiettyjä toimenpiteitä. Ne saavat käyttää ilmoitusta tietolähteenä omiin tarkoituksiinsa.

Kyseiset viranomaiset voidaan lisäksi eriyttää sen mukaan, voivatko ne käyttää tietoja omiin tarkoituksiinsa tiettyä tavoitetta varten vai voivatko ne (lähinnä Europol ja Eurojust) käyttää tietoja omiin tarkoituksiinsa ilman, että käyttötarkoitusta tarvitsee mitenkään eritellä. Turvapaikkaviranomaiset voivat esimerkiksi käyttää tietoja tiettyyn tarkoitukseen, vaikka se ei olisikaan ilmoituksessa mainittu tarkoitus. Niillä on oikeus käyttää maahanmuuttotietoja ”sen määrittämiseksi, onko turvapaikan hakija oleskellut luvatta toisessa jäsenvaltiossa”. Europolilla ja Eurojustilla on kuitenkin oikeus käyttää tiettyihin ilmoitusluokkiin sisältyviä tietoja, jotka ovat tarpeen niiden tehtävien suorittamiseksi.

Yhteenvetona voidaan todeta, että oikeus käyttää SIS II-tietoja myönnetään kolmessa tapauksessa:

— oikeus käyttää tietoja ilmoituksen tekemistä varten;

— oikeus käyttää tietoja muuhun tarkoitukseen kuin SIS II:ta varten, jotka on kuitenkin ehdotuksissa tarkasti rajattu;

— oikeus käyttää tietoja muuhun tarkoitukseen kuin SIS II:ta varten, joita ei ole kuvattu täsmällisesti.

Tietosuojavaltuutettu katsoo, että mitä yleisempi tietojen käyttötarkoitus, sitä tiukempia tarvittavien suojatoimien olisi oltava. Jäljempänä esitetään yksityiskohtaisesti yleiset suojatoimet, minkä jälkeen käsitellään Europolin ja Eurojustin erityistilannetta.

4.2.2 *Käyttöoikeuden antamisedellytykset*

1. Käyttöoikeus voidaan antaa kaikissa tapauksissa vain, jos se soveltuu SIS II:n yleiseen tarkoitukseen ja on johdonmukainen sen oikeusperustan kanssa.

Käytännössä tämä tarkoittaa sitä, että asetusehdotuksen mukaisen maahanmuuttotietojen käyttöoikeuden on tuettava henkilöiden liikkuvuutta koskevaan Schengenin säännöstön osaan liittyvien politiikkojen toteuttamista.

Vastaavasti päätösehdotukseen sisältyvien ilmoitusten käytöllä on pyrittävä tukemaan poliisi- ja oikeusviranomaisten operatiivista yhteistyötä rikosasioissa.

Tietosuojavaltuutettu kiinnittää tässä suhteessa huomiota lukuun, joka koskee rekisteröintitodistusten myöntämisestä vastaavien viranomaisten oikeutta käyttää SIS II:ta (ks. 4.6 kohta jäljempänä).

2. Tarve käyttää SIS II:n tietoja on osoitettava samoin kuin se, että tietojen saanti muulla, vähemmän tunkeilevalla tavalla on joko mahdotonta tai erittäin vaikeaa. Tämä olisi pitänyt esittää perusteluissa, joiden puuttuminen on, kuten jo aiemmin mainittiin, erittäin valitettavaa.

3. Tietojen käyttötarkoitus on määriteltävä yksiselitteisesti ja rajoittavasti.

Esimerkiksi turvapaikkaviranomaisilla on oikeus käyttää maahanmuuttotietoja ”sen määrittämiseksi, onko turvapaikan hakija oleskellut luvatta toisessa jäsenvaltiossa”. Europol ja Eurojust voivat kuitenkin käyttää tiettyihin tietoluokkiin sisältyviä tietoja, jotka ovat tarpeen niiden tehtävien suorittamiseksi. Tämä ei ole riittävän yksityiskohtainen rajoitus (ks. jäljempänä).

4. Käyttöoikeuden myöntämisedellytykset on määriteltävä ja rajattava tarkasti. Oikeus olisi annettava erityisesti vain niille kyseisten organisaatioiden yksiköille, jotka joutuvat käsittelemään SIS II -tietoja. Tätä velvoitetta, josta säädetään päätösehdotuksen 40 artiklassa ja asetusehdotuksen 21 artiklan 2 kohdassa, olisi täydennettävä kansallisten viranomaisten velvoitteella pitää ajantasaista luetteloa henkilöistä, joilla on oikeus käyttää SIS II:ta. Europolilla ja Eurojustilla olisi oltava vastaava velvoite.

5. Se, että kyseisille viranomaisille on annettu oikeus käyttää SIS II-tietoja, ei voi koskaan olla peruste tallentaa tai säilyttää tietoja järjestelmässä, jos niistä ei ole hyötyä tietylle ilmoitukselle, johon ne kuuluvat. Uusia tietoluokkia ei saa lisätä sen vuoksi, että niistä olisi hyötyä muille tietojärjestelmille. Päätösehdotuksen 39 artiklassa esimerkiksi säädetään ilmoituksen tekevää viranomaista koskevien tietojen lisäämisestä ilmoitukseen. Kyseisiä tietoja ei tarvita toimenpiteen toteuttamiseen (esim. pidätys tai valvonta), ja ainoa syy, miksi ne lisättäisiin, on todennäköisesti se, että siitä olisi hyötyä Europolille tai Eurojustille. Kyseisten tietojen käsittelylle olisikin lisättävä selkeät perustelut.

6. Tietojen säilyttämisaikaa ei saa jatkaa, ellei tarkoitus, jota varten tiedot tallennettiin, sitä edellytä. Tämä tarkoittaa sitä, että vaikka Europol ja Eurojust voisivatkin käyttää kyseisiä tietoja, se ei kuitenkaan ole riittävä peruste säilyttää niitä järjestelmässä (esimerkiksi etsityn henkilön luovuttamisen jälkeen tiedot olisi poistettava, vaikka niistä olisi hyötyä Europolille). Huolellisen valvonnan avulla on jälleen kerran varmistettava, että kansalliset viranomaiset noudattavat tätä vaatimusta.

4.2.3 *Europolin ja Eurojustin pääsy järjestelmään*

a. *Järjestelmään pääsyn perusteet*

Europolin ja Eurojustin pääsystä joihinkin SIS-tietoihin on keskusteltu jo ennen niiden ottamista mukaan 24.2.2005 annetulla neuvoston päätöksellä ([1]). Niille on myönnetty kaikkein avoimin pääsy järjestelmään kaikkien niiden viranomaisten piirissä, jotka voivat päästä järjestelmään omia tarkoitusperiään varten. Vaikka kyseisten tietojen käyttöä on kuvailtu päätöksen XII luvussa, järjestelmään pääsyn myöntämisen perusteita ei ole alun pitäenkään eritelty riittävästi. Näin on varsinkin ottaen huomioon, että Europolin ja Eurojustin tehtävät todennäköisesti kehittyvät ajan mittaan.

Euroopan tietosuojavaltuutettu kehottaa komissiota rajaamaan ne tehtävät, joiden suorittamiseen käyttöoikeuden myöntäminen Europolille ja Eurojustille olisi perusteltua.

b. *Tietoja koskevat rajoitukset*

Europolin ja Eurojustin suorittaman ”tietojenonginnan” välttämiseksi ja sen varmistamiseksi, että niillä on pääsy vain ”niiden tehtävien kannalta välttämättömiin” tietoihin, Schengenin yhteinen valvontaviranomainen ehdotti SIS II -ehdotuksista 27.9.2005 antamassaan lausunnossa, että Europolin ja Eurojustin pääsy järjestelmään rajoitettaisiin tietoihin henkilöistä, joiden nimi jo ilmenee niiden tiedostoissa. Tämä takaisi, että ne konsultoivat ainoastaan niiden kannalta relevantteja ilmoituksia. Euroopan tietosuojavaltuutettu kannattaa tätä suositusta.

c. *Turvallisuusnäkökohdat*

Euroopan tietosuojavaltuutettu suhtautuu myönteisesti velvoitteeseen rekisteröidä järjestelmään kaikki Europolin ja Eurojustin suorittamat tapahtumat sekä järjestelmän osien kopioinnin tai lataamisen kieltämiseen.

Ehdotetun päätöksen 56 artiklassa kaavaillaan ”yhdestä kahteen” käyttöliittymää Europolia ja Eurojustia varten. Vaikka olisikin ymmärrettävää, että jokin jäsenvaltio tarvitsee enemmän kuin yhden käyttöliittymän sen toimivaltaisten viranomaisten hajautetun tilanteen takia, Europolin ja Eurojustin asema ja toiminnot eivät oikeuta tätä pyyntöä. Lisäksi on korostettava, että turvallisuusnäkökulmasta käyttöliittymien lisääminen lisää myös väärinkäytön riskiä, ja se olisi siksi perusteltava täsmällisesti pätevämpien tekijöiden avulla. Näin ollen vakuuttavampien perustelujen puuttuessa Euroopan tietosuojavaltuutettu ehdottaa, että Europolin ja Eurojustin osalta myönnetään vain yksi käyttöliittymä.

4.3 **Ilmoitusten linkittäminen**

Asetuksen 26 artiklassa ja päätöksen 46 artiklassa säädetään, että jäsenvaltiot voivat luoda kansallisen lainsäädäntönsä mukaisesti ilmoitusten välille linkkejä, yhdistääkseen kaksi tai useampia ilmoituksia.

Vaikka ilmoitusten väliset linkit ovat epäilemättä hyödyllisiä valvonnan kannalta (esimerkiksi autovarkaan pidätysmääräys voidaan linkittää varastettuun ajoneuvoon), ilmoitusten välisten linkkien käyttöönotto on hyvin tyypillinen poliisin tutkintakeinon piirre.

Ilmoitusten linkittämisellä voi olla suuri vaikutus kyseisen henkilön oikeuksiin, koska henkilöä ei enää arvioida ainoastaan häneen liittyvien tietojen perustella, vaan sen perusteella, mikä on hänen mahdollinen yhteytensä muihin henkilöihin. Henkilöihin, joiden tiedot linkitetään rikollisten tai etsintäkuulutettujen tietoihin, kohdistuu todennäköisesti suurempi epäily kuin muihin. Lisäksi ilmoitusten linkittäminen merkitsee SIS:n tutkintavaltuuksien laajentamista, koska se mahdollistaa oletettujen järjestöjen tai verkostojen rekisteröinnin (esimerkiksi jos laittomia maahanmuuttajia koskevat tiedot linkitetään ihmiskaupan harjoittajien tietoihin). Koska linkkien luominen jätetään kansallisen lainsäädännön varaan, siitä on lopuksi mahdollisena seurauksena se, että jokin jäsenvaltio voi luoda linkkejä, jotka jossakin toisessa jäsenvaltiossa ovat lainvastaisia, syöttäen näin järjestelmään ”lainvastaisia” tietoja.

([1]) Neuvoston päätös 2005/211/YOS, tehty 24 päivänä helmikuuta 2005, Schengenin tietojärjestelmän eräiden uusien toimintojen käyttöönottamisesta, myös terrorismin torjunnassa. EUVL L 68, 15.3.2005, s. 44.

Neuvoston 14.6.2004 antamissa SIS II:n toiminnallisia vaatimuksia koskevissa päätelmissä todettiin, että kuhunkin linkkiin on liityttävä selvät toiminnalliset vaatimukset, niiden on perustuttava selkeästi määriteltyyn yhteyssuhteeseen ja niiden on noudatettava suhteellisuusperiaatetta. Linkittämisellä ei saa myöskään olla vaikutusta oikeuteen päästä järjestelmään. Koska ilmoitusten linkittäminen on kuitenkin tietojen käsittelyä, siinä on noudatettava direktiivin 95/46/EY ja/tai yleissopimuksen N:o 108 täytäntöönpanemiseksi annetun kansallisen lainsäädännön säännöksiä.

Ehdotuksissa toistetaan, että linkkien olemassaolo ei voi muuttaa järjestelmään pääsyn oikeuksia (sillä muutoinhan se tarjoaisi pääsyn tietoihin, joiden käsittely ei olisi kansallisen lainsäädännön nojalla laillista, rikkoen direktiivin 6 artiklaa vastaan).

Euroopan tietosuojavaltuutettu korostaa, että ehdotetun asetuksen 26 artiklan ja ehdotetun päätöksen 46 artiklan tiukka tulkinta on tärkeää: yksi keino tämän varmistamiseksi on tehdä selväksi, että viranomaiset, joilla ei ole oikeutta päästä tiettyihin tietoluokkiin, eivät voi päästä näihin luokkiin kuuluviin linkkeihin eivätkä ne saa edes olla tietoisia kyseisten linkkien olemassaolosta. Linkkien havaitsemisen on oltava mahdotonta niille, joilla ei ole käyttöoikeutta linkitettyihin tietoihin.

Lisäksi Euroopan tietosuojavaltuutettu haluaisi, että häntä kuultaisiin teknisistä toimenpiteistä tämän takaamiseksi.

4.4 **Ilmoitukset maahantulon epäämiseksi**

4.4.1 *Tietojen tallentamisen perusteet*

Maahantulon epäämiseksi annettujen kolmansien maiden kansalaisia koskevien ilmoitusten (asetuksen 15 artikla) käytöllä on merkittävä vaikutus henkilön vapauksiin: tämän säännöksen nojalla raportoinnin kohteena oleva yksittäinen henkilö ei voi enää päästä Schengen-alueelle useaan vuoteen. Tähän mennessä tämä ilmoitustyyppi on ollut kaikkein eniten käytetty, raportoinnin kohteena olevien henkilöiden määrissä laskettuna. Ottaen huomioon tämän ilmoituksen seuraukset sekä asianomaisten henkilöiden määrän, ilmoitusta tehtäessä sekä täytäntöön pantaessa on syytä erityiseen huolellisuuteen. Vaikka sama koskee muitakin ilmoituksia, Euroopan tietosuojavaltuutettu aikoo omistaa erityisen luvun tälle ilmoitukselle, koska siitä aiheutuu tietojen tallentamisen perusteita koskevia erityisongelmia.

Uusi ilmoitus maahantulon epäämiseksi merkitsee parannusta nykyiseen tilanteeseen, mutta se ei kuitenkaan ole täysin tyydyttävä, sillä se perustuu suurelta osin välineisiin, joita ei ole vielä hyväksytty tai edes ehdotettu.

Parannusta on täsmällisempi kuvaus tietojen tallentamisen perusteista. Schengenin yleissopimuksen nykyinen sanamuoto on johtanut siihen, että jäsenvaltioiden välillä on ollut suuria eroja raportoinnin kohteena yleissopimuksen 96 artiklan nojalla olleiden henkilöiden määrissä. Schengenin yhteinen valvontaviranomainen on laatinut perusteellisen tutkimuksen asiasta ([1]) ja päätynyt suositukseen, jonka mukaan ”päätöksentekijöiden olisi harkittava ilmoituksen tekemisen syiden yhdenmukaistamista eri Schengen-valtioissa”.

Ehdotettu 15 artikla on sanamuodoltaan yksityiskohtaisempi, mikä on myönteistä.

Lisäksi 15 artiklan 2 kohdassa annetaan luettelo tapauksista, joissa henkilöistä ei voida tehdä ilmoitusta, koska he oleskelevat laillisesti jonkin jäsenvaltion alueella, erilaisia asemia soveltaen. Vaikka tämä voidaan päätellä nykyisestä Schengenin yleissopimuksesta, käytäntö on osoittanut, että tämän menettelyn soveltaminen on vaihdellut eri jäsenvaltioissa. Sen vuoksi selkeyttäminen on positiivinen tekijä.

Tätä säännöstä on kuitenkin myös kritisoitu vahvasti, koska se perustuu suurelta osin tekstiin, jota ei ole vielä hyväksytty, nimittäin palauttamista koskevaan direktiiviin.

SIS II -ehdotusten hyväksymisen jälkeen komissio on ehdottanut (1.9.2005) direktiiviä jäsenvaltioissa sovellettavista yhteisistä vaatimuksista ja menettelyistä palautettaessa laittomasti oleskelevia kolmansien maiden kansalaisia, mutta niin kauan kuin tämä ehdotus ei ole lopullinen, sitä ei voida pitää pätevänä perusteena tietojen tallentamiselle järjestelmään. Se rikkoo erityisesti ECHR:n 8 artiklaa vastaan, sillä henkilöiden yksityisyyden loukkaaminen olisi perusteltava — muun muassa — selkeän ja saatavissa olevan lainsäädännön avulla.

Näistä syistä Euroopan tietosuojavaltuutettu kehottaa komissiota joko poistamaan tämän säännöksen tai muotoilemaan sen olemassaolevaan lainsäädäntöön perustuen uudelleen siten, että henkilöillä on mahdollisuus tietää, mitä toimenpiteitä viranomaiset voivat tarkalleen toteuttaa heidän osaltaan.

4.4.2 *Oikeus käyttää 15 artiklan mukaisia ilmoituksia*

Asetuksen 18 artiklassa säädetään, millä viranomaisilla on oikeus käyttää kyseisiä ilmoituksia ja mihin tarkoituksiin. 18 artiklan 1 ja 2 kohdassa määritetään viranomaiset, joilla on oikeus käyttää palauttamista koskevan direktiivin perusteella tehtyjä ilmoituksia. Aikaisemmin esitetty huomautus soveltuu tähänkin kohtaan.

([1]) Schengenin yhteisen valvontaviranomaisen kertomus 96 artiklan mukaisten ilmoitusten käytön tarkastelusta Schengenin tietojärjestelmässä, Bryssel, 20.6.2005.

Ehdotetun asetuksen 18 artiklan 3 kohdassa pakolaisaseman myöntämisestä vastuussa oleville viranomaisille myönnetään oikeus käyttää ilmoituksia sellaisen direktiivin nojalla, jota ei ole vielä edes ehdotettu. Käytettävissä olevan tekstin puuttuessa Euroopan tietosuojavaltuutetun on toistettava aikaisemmat huomautukset.

4.4.3 *15 artiklan mukaisten ilmoitusten säilyttämisaika*

Ilmoitusta ei 20 artiklan mukaisesti saa säilyttää (maastapoistamista tai palauttamista koskevassa) päätöksessä vahvistettua maahantulokiellon kestoa kauempaa. Tämä on tietosuojasääntöjen mukaista. Lisäksi ilmoitus poistetaan automaattisesti viiden vuoden kuluttua, mikäli tiedot SIS II:een tallentanut jäsenvaltio ei päätä toisin.

Asianmukaisen kansallisen tason valvonnan avulla olisi varmistettava, että säilyttämisaikaa ei perusteetta jatketa automaattisesti ja että jäsenvaltiot poistavat tiedot ennen viiden vuoden määräaikaa, jos maahantulokiellon kesto on lyhyempi.

4.5 **Säilyttämisajat**

Vaikka säilyttämisen periaate pysyy samana (yleensä ilmoitus olisi poistettava SIS II -järjestelmästä heti, kun ilmoituksessa pyydetty toimenpide on suoritettu), ehdotukset johtavat siihen, että ilmoitusten säilyttämisajan voimassaoloa on yleensä pidennetty.

Schengenin yleissopimuksessa määrättiin, että tietojen säilyttämistarve on tarkistettava viimeistään kolmen vuoden kuluttua niiden tallentamisesta (tai yhden vuoden kuluttua, kun tiedot on tallennettu tarkkailua varten). Uusissa ehdotuksissa säädetään tietojen automaattisesta poistamisesta (jota ilmoituksen tehneellä jäsenvaltiolla on mahdollisuus vastustaa) 5 vuoden kuluttua maahanmuuttotietojen osalta, 10 vuoden kuluttua pidätystä, kadonneita henkilöitä ja henkilöitä, jotka on haastettu oikeuteen, koskevien tietojen osalta sekä 3 vuoden kuluttua tarkkailtavien henkilöiden osalta.

Vaikka jäsenvaltioiden on periaatteessa poistettava tiedot, kun ilmoituksen tarkoitus on täytetty, tämä johtaa säilyttämistä koskevan enimmäisajan merkittävään pitenemiseen (useimmissa tapauksissa kolminkertaistumiseen), ilman minkäänlaisia komission perusteluja. Maahanmuuttotietojen osalta voidaan vain uskaltaa arvata, että 5 vuoden kesto on yhteydessä maahantulokiellon kestoon, kuten palauttamista koskevassa direktiiviehdotuksessa on ehdotettu. Muissa tapauksissa ei ole olemassa mitään järkevää perustetta, josta Euroopan tietosuojavaltuutettu olisi tietoinen.

Mahdolliset vaikutukset rekisteröityihin, jotka ovat SIS:ssä raportoinnin kohteena, voivat johtaa merkittäviin seurauksiin asianomaisten henkilöiden elämässä. Tämä on huolestuttavaa erityisesti, kun henkilöistä on annettu ilmoitus tarkkailua tai erityistarkastuksia varten, koska nämä ilmoitukset voidaan antaa epäilysten perusteella.

Euroopan tietosuojavaltuutettu kaipaa vankkoja perusteluja kyseiselle tietojen säilyttämisaikojen voimassaolon pidentämiselle. Mikäli vakuuttavia perusteluja ei ole, hän ehdottaa niiden lyhentämistä nykyiseen kestoonsa, erityisesti silloin, kun kyseessä ovat ilmoitukset tarkkailua tai erityistarkastuksia varten.

4.6 **Ajoneuvojen rekisteröintitodistusten myöntämisestä vastaavien viranomaisten pääsy järjestelmään**

Pääongelmana on enemmän kuin kyseenalaisen oikeusperustan valinta. Komissio ei perustele vakuuttavasti ”liikennettä” koskevan ensimmäisen pilarin oikeusperustan käyttämistä sellaista toimenpidettä varten, jolla sallittaisiin hallintoviranomaisten pääsy SIS-järjestelmään rikollisuuden ehkäisemiseksi ja torjumiseksi (varastettujen ajoneuvojen laiton kauppa). Tämän lausunnon 4.2.2 kohdassa on esitetty yksityiskohtaisesti, että tarvitaan vahvoja perusteluja ja vankkaa oikeusperustaa, jotta pääsy SIS II -järjestelmään myönnettäisiin.

Euroopan tietosuojavaltuutettu viittaa asiaa koskeviin huomautuksiin, jotka Schengenin yhteinen valvontaviranomainen on esittänyt lausunnossaan ehdotetusta SIS II:n oikeusperustasta. Erityisesti Schengenin yhteisen valvontaviranomaisen ehdotusta päätösehdotuksen muuttamisesta kyseisen pääsyn sisällyttämiseksi siihen olisi noudatettava.

5. **KOMISSION JA JÄSENVALTIOIDEN TEHTÄVÄT**

Selkeä vastuualueiden kuvaus ja vastuunjako on SIS II:n yhteydessä ensiarvoisen tärkeää sekä järjestelmän moitteettoman toiminnan kannalta että myös valvonnan näkökulmasta. Valvontavaltuuksien jakaminen nojaa vastuualueiden kuvaukseen, joten ehdoton selkeys on välttämätöntä.

5.1 **Komission tehtävä**

Euroopan tietosuojavaltuutettu suhtautuu myönteisesti molempien ehdotusten III lukuun, jossa määritetään komission tehtävä ja vastuualueet SIS II:ssa (tehtävänä operatiivinen hallinnointi). Tällaista selvennystä ei ollut VIS-ehdotuksessa. Mainitussa luvussa ei kuitenkaan määritellä tyhjentävästi komission tehtäviä. Kuten tämän lausunnon 9 luvussa todetaan, komissio osallistuu järjestelmän täytäntöönpanoon ja hallinnointiin myös komiteamenettelyn kautta.

Tietosuojan kannalta komissiolla on tehtävä, joka on jo tunnustettu VIS- ja Eurodac-järjestelmissä, eli operatiivisesta hallinnoinnista vastaaminen. Yhdistettynä sen päätehtävään järjestelmän kehittämisessä ja ylläpidossa tätä olisi pidettävä sui generis -rekisterinpitäjän tehtävänä. Kuten Euroopan tietosuojavaltuutetun lausunnossa VIS-järjestelmästä on jo todettu, se on paljon enemmän kuin tietojenkäsittelijän tehtävä, mutta myös rajatumpi kuin normaalin rekisterinpitäjän, sillä komissiolla ei ole pääsyä SIS II:ssa käsiteltyihin tietoihin.

Koska SIS II perustetaan monitahoisille järjestelmille, joista eräät nojaavat uusiin teknologioihin, Euroopan tietosuojavaltuutettu korostaa komission vastuun vahvistamista järjestelmien pitämisessä ajan tasalla, soveltamalla turvallisuuteen ja tietosuojaan liittyviä parhaita käytettävissä olevia tekniikoita.

Näin ollen ehdotusten 12 artiklaan olisi lisättävä, että komission olisi säännöllisesti ehdotettava sellaisten uusien teknologioiden soveltamista, jotka edustavat uusinta tietämystä ja jotka parantavat tietosuojan ja turvallisuuden tasoa sekä helpottavat niiden kansallisten viranomaisten tehtäviä, joilla on pääsy näihin tietoihin.

5.2 **Jäsenvaltioiden tehtävä**

Jäsenvaltioiden tilanne ei ole kovin selkeä, koska on vaikea tietää, mikä tai mitkä viranomaiset tulevat olemaan rekisterinpitäjiä.

Ehdotuksissa määritetään SIS II:n kansallisen toimiston tehtävä (varmistaa, että toimivaltaiset viranomaiset pääsevät SIS II:een) sekä SIRENE-viranomaisten tehtävä (huolehtia kaikkien lisätietojen vaihdosta). Jäsenvaltioiden on myös taattava NS:iensä (kansallisten järjestelmiensä) toiminta ja turvallisuus. Ei ole selvää, kuuluuko tämä vastuu yhdelle edellä mainituista viranomaisista. Joka tapauksessa selkeytystä tarvitaan tältä osin.

Tietosuojan osalta komissiota ja jäsenvaltioita olisi pidettävä yhteisinä rekisterinpitäjinä, joista kullakin on erityinen vastuualue. Näiden täydentävien tehtävien tunnustaminen on ainoa tapa varmistaa, ettei yksikään SIS II:n toimintojen alue jää valvomatta.

6. **REKISTERÖITYJEN OIKEUDET**

6.1 **Tiedot**

6.1.1 *Asetusehdotus*

Asetusehdotuksen 28 artiklassa säädetään rekisteröidyn tietojensaantioikeudesta, joka perustuu pitkälti direktiivin 95/46 10 artiklaan. Tämä on tervetullut muutos verrattuna nykytilanteeseen, sillä yleissopimuksessa ei säädetä yksiselitteisesti tietojensaantioikeudesta. Seuraavia seikkoja olisi kuitenkin vielä mahdollista parantaa.

Luetteloon olisi lisättävä joitakin tietoja, millä varmistettaisiin rekisteröidyn oikeudenmukainen kohtelu ([1]). Tietojen olisi koskettava tietojen säilyttämisaikaa, oikeutta pyytää ilmoituksen tekemistä koskevan päätöksen tarkastelua tai hakea siihen muutosta (joissakin tapauksissa ks. asetusehdotuksen 15 artiklan 3 kohta), mahdollisuutta saada apua tietosuojaviranomaiselta ja oikeuskeinojen olemassaolo.

Asetusehdotuksessa ei täsmennetä, milloin tiedot olisi toimitettava. Tämä voi tehdä rekisteröidyn oikeuksien käytön mahdottomaksi. Jotta oikeuksia voidaan todellisuudessa käyttää, asetuksessa olisi säädettävä tarkasti ajankohta, jona tiedot olisi annettava riippuen siitä, mikä viranomainen on tehnyt ilmoituksen.

Käytännöllinen ratkaisu olisi lisätä ilmoitusta koskevia tietoja ilmoituksen ensisijaisena perusteena olevaan päätökseen. Tällainen päätös on joko tuomioistuimen päätös tai hallinnollinen päätös, joka perustuu yleistä turvallisuutta koskevaan uhkaan (…), palautuspäätökseen tai maastapoistamispäätökseen, johon liittyy uutta maahantuloa koskeva kielto. Tämä seikka olisi lisättävä asetuksen 28 artiklaan.

6.1.2 *Päätösehdotus*

Päätöksen 50 artiklan mukaan tietoja annetaan rekisteröidyn pyynnöstä, ja siinä annetaan mahdolliset perusteet tietojen luovuttamisesta kieltäytymiselle. Tietojensaantioikeutta koskevat rajoitukset ovat luonnollisesti ymmärrettäviä ottaen huomioon tietojen luonteen ja sen, missä yhteydessä niitä käsitellään.

Tietojensaantioikeuden edellytyksenä ei kuitenkaan pitäisi olla rekisteröidyn tekemä pyyntö (joka olisi pikemminkin tietojensaantipyyntöä koskeva määritelmä). Voidaan olettaa, että tarve ”pyytää” tietoja on perusteltu tapauksissa, joissa rekisteröidylle ei voida ilmoittaa sen vuoksi, että hänen olinpaikkaansa ei tunneta.

Tämä asia voitaisiin ottaa huomioon lisäämällä tietojensaantioikeutta koskeva poikkeus tapauksissa, joissa tietojen toimittaminen osoittautuu mahdottomaksi tai siitä aiheutuu suhteettoman suurta vaivaa. Päätöksen 50 artiklaa olisi muutettava vastaavasti.

([1]) Ks. myös tietosuojavaltuutetun lausunto viisumitietojärjestelmän perustamisesta, kohta 3.10.1.

Ratkaisu olisi myös johdonmukainen tietosuojaa kolmannessa pilarissa koskevan puitepäätösehdotuksen kanssa.

6.2 **Tietojen saanti**

Myönteistä on, että sekä asetus- että päätösehdotuksessa asetetaan määräajat tietojen saantipyyntöihin vastaamiseksi. Koska tietojensaantioikeuden käyttöä koskeva menettely määräytyy kansallisella tasolla, voidaan kuitenkin kysyä, miten ehdotuksissa säädetyt määräajat vaikuttavat olemassa oleviin menettelyihin etenkin, jos jäsenvaltioilla on lyhyemmät määräajat tietojensaantipyyntöihin vastaamiseksi. Olisi todettava selkeästi, että olisi sovellettava rekisteröidyn kannalta suotuisampia määräaikoja.

6.2.1 *Asetusehdotus*

On huomattava, asetusehdotus ei sisällä tietojensaantioikeutta koskevia rajoituksia (…kieltäydytään, mikäli se on välttämätöntä ilmoituksessa mainitun oikeudellisen toimenpiteen suorittamiseksi tai muiden henkilöiden oikeuksien tai vapauksien suojelemiseksi), jotka nykyisellään sisältyvät Schengenin yleissopimukseen.

Tämä johtunee kuitenkin direktiivistä 95/46/EY, jossa (13 artiklassa) säädetään jäsenvaltioiden mahdollisuudesta toteuttaa poikkeuksia kansallisessa lainsäädännössä. Joka tapauksessa on todettava, että käytettäessä 13 artiklaa kansallisessa lainsäädännössä tiedonsaantioikeuden rajoittamiseksi olisi aina otettava huomioon Euroopan ihmisoikeussopimuksen 8 artikla ja että sitä olisi käytettävä vain rajoitetusti.

6.2.2 *Päätösehdotus*

Päätösehdotus sisältää Schengenin yleissopimuksen kaltaisen rajoituksen tietojensaantioikeuteen. Puitepäätösehdotus sisältää pohjimmiltaan samat rajoitukset, joten tämän säädöksen antaminen ei muuttaisi tilannetta merkittävästi.

Useissa jäsenvaltioissa oikeus saada lainvalvontatietoja on ”epäsuora” (eli oikeutta voidaan käyttää kansallisen tietosuojaviranomaisen välityksellä), minkä vuoksi olisi hyödyllistä säätää tietosuojaviranomaisten velvoitteesta tehdä aktiivista yhteistyötä käytettäessä tietojensaantioikeutta.

6.3 **Oikeus saattaa ilmoituksen tekemistä koskeva päätös tarkasteltavaksi tai hakea siihen muutosta**

Asetuksen 15 artiklan 3 kohdassa säädetään oikeudesta saattaa asia oikeusviranomaisen tarkasteltavaksi tai hakea muutosta oikeusviranomaiselta, jos ilmoituksen tekemisestä päättää hallintoviranomainen. Tämä on tervetullut lisä verrattuna nykyiseen Schengenin yleissopimukseen.

Tämä korostaa edellä 6.1 kohdassa mainitun mukaisesti täydellisten ja ajantasaisten tietojen merkitystä rekisteröidylle. Ilman kyseisiä tietoja uusi oikeus jäisi teoreettiseksi.

6.4 **Oikeuskeinot**

Asetusehdotuksen 30 artiklassa ja päätösehdotuksen 52 artiklassa säädetään oikeudesta nostaa kanne tai tehdä kantelu minkä tahansa jäsenvaltion tuomioistuimissa, jos rekisteröidyltä evätään oikeus tutustua itseään koskeviin tietoihin tai oikaista niitä tai poistaa ne taikka oikeus tiedoksisaantiin tai vahingonkorvaukseen.

Ilmaisu ”kenellä tahansa on oltava kussakin jäsenvaltiossa” antaa ymmärtää, että kanteen tekijän on oltava fyysisesti jäsenvaltion alueella voidakseen nostaa kanteensa tuomioistuimessa. Kyseinen alueellinen rajoitus ei ole perusteltu ja se voi mitätöidä mahdollisuuden oikeuskeinojen käyttöön, koska on todennäköistä, että hyvin usein kanteen tekijä jättää kanteen nimenomaan siksi, että hänelle ei myönnetä pääsyä Schengenin alueelle. Lisäksi asetusehdotuksen osalta on huomattava, että koska direktiivi on yleinen sääntö (lex generalis), on sen 22 artikla otettava huomioon. Kyseisen artiklan mukaan kenellä tahansa henkilöllä on mahdollisuus käyttää oikeussuojakeinoa asuinpaikastaan riippumatta. Puitepäätösehdotuksessa ei ole myöskään alueellista rajoitusta. Tietosuojavaltuutettu ehdottaakin, että alueellinen rajoitus poistettaisiin asetusehdotuksen 30 artiklasta ja päätösehdotuksen 52 artiklasta.

7. **VALVONTA**

7.1 **Johdanto: vastuun jakaminen**

Ehdotuksissa valvontatehtävä jaetaan kansallisten valvontaviranomaisten ([1]) ja Euroopan tietosuojavaltuutetun kesken kummankin omalla soveltamisalalla. Tämä on yhdenmukaista ehdotuksissa omaksutun sovellettavaa lainsäädäntöä ja SIS II:n toimintaan ja käyttöön liittyvää vastuuta koskevan lähestymistavan sekä tehokkaan valvonnan vaatimuksen kanssa.

Tietosuojavaltuutettu on tyytyväinen tähän asetusehdotuksen 31 artiklassa ja päätösehdotuksen 53 artiklassa esitettyyn lähestymistapaan. Eri osapuolten tehtävien ymmärtämiseksi ja selkeyttämiseksi tietosuojavaltuutettu ehdottaa kuitenkin, että artiklat jaettaisiin useampaan säännökseen, joista kukin käsittelisi valvonnan eri tasoa samalla tavalla kuin VIS-ehdotuksessa.

([1]) Myös Europolin ja Eurojustin valvontaviranomaiset osallistuvat valvontaan mutta vähemmässä määrin.

7.2 **Kansallisten tietosuojaviranomaisten suorittama valvonta**

Asetusehdotuksen 31 artiklan ja päätösehdotuksen 53 artiklan mukaan kunkin jäsenvaltion on huolehdittava siitä, että riippumaton viranomainen valvoo SIS II -järjestelmään sisältyvien henkilötietojen käsittelyn lainmukaisuutta.

Päätösehdotuksen 53 artiklassa säädetään yksilön oikeudesta pyytää valvontaviranomaista tarkistamaan häntä koskevien tietojen käsittelyn lainmukaisuus. Asetusehdotuksessa ei ole samanlaista säännöstä, koska direktiiviä sovelletaan yleisenä sääntönä (*lex generalis*). Siksi on otettava huomioon, että kansalliset tietosuojaviranomaiset voivat käyttää SIS II:n osalta kaikkia niille direktiivin 95/46/EY 28 artiklan nojalla annettuja toimivaltuuksia, tietojenkäsittelyn lainmukaisuuden tarkistaminen mukaan luettuna. Asetuksen 31 artiklan 1 kohdassa selvennetään kansallisten viranomaisten tehtävää, mutta sitä ei voida tulkita niiden toimivaltuuksia rajoittavasti. Asetusehdotuksen tekstiä olisi selvennettävä toimivaltuuksien kuvauksen osalta.

Päätösehdotuksessa kansallisten valvontaviranomaisten tehtävät on kuvattu laajemmin, koska sen *lex generalis* on eri. Tilanne, jossa valvontaviranomaisilla olisi eri tehtävät ja eri toimivaltuudet käsiteltävänä olevien tietojen luokituksesta riippuen, ei kuitenkaan olisi järkevä, minkä lisäksi sitä olisi vaikea hallinnoida käytännössä. Siksi sitä olisi vältettävä joko antamalla näille viranomaisille samat toimivaltuudet päätösehdotuksen tekstissä tai viittaamalla toiseen yleiseen sääntöön (puitepäätökseen tietosuojasta kolmannen pilarin aloilla), jossa tietosuojaviranomaisille annetaan enemmän toimivaltaa.

7.3 **Euroopan tietosuojavaltuutetun suorittama valvonta**

Euroopan tietosuojavaltuutettu valvoo, että komission tietojenkäsittelytoiminta toteutetaan ehdotusten mukaisesti. Lisäksi tietosuojavaltuutetun pitäisi voida käyttää kaikkia asetuksen 45/2001 nojalla annettuja toimivaltuuksiaan ottaen kuitenkin huomioon komission rajalliset toimivaltuudet itse tietojen osalta.

On aiheellista lisätä, että asetuksen 45/2001 45 artiklan f kohdan mukaan Euroopan tietosuojavaltuutettu ”tekee yhteistyötä direktiivin 95/46/EY 28 artiklassa mainittujen, kyseisen direktiivin soveltamisalaan kuuluvien maiden kansallisten valvontaviranomaisten kanssa siinä määrin kuin kullekin viranomaiselle kuuluvien tehtävien hoitaminen sitä edellyttää”. SIS II:n valvontaan liittyvä yhteistyö jäsenvaltioiden kanssa ei perustu ainoastaan ehdotuksiin vaan myös asetukseen 45/2001.

7.4 **Yhteinen valvonta**

Ehdotuksissa on otettu huomioon myös tarve koordinoida eri viranomaisten valvontatoimet. Asetusehdotuksen 31 artiklassa ja päätösehdotuksen 53 artiklassa säädetään, että ”kansallisten valvontaviranomaisten ja Euroopan tietosuojavaltuutetun on tehtävä keskenään aktiivista yhteistyötä. Euroopan tietosuojavaltuutetun on järjestettävä tätä tarkoitusta varten kokous vähintään kerran vuodessa.”

Euroopan tietosuojavaltuutettu on tyytyväinen tähän ehdotukseen, joka sisältää olennaisilta osin ne osatekijät, jotka ovat tarpeen tämän ehdottoman välttämättömän yhteistyön mahdollistamiseksi valvonnasta vastaavien viranomaisten välillä kansallisella ja Euroopan tasolla. On syytä korostaa, että kun ehdotuksissa säädetään vähintään kerran vuodessa pidettävästä kokouksesta, tätä on pidettävä vähimmäisvaatimuksena.

Näitä säännöksiä (asetusehdotuksen 31 artiklaa ja päätösehdotuksen 53 artiklaa) voitaisiin kuitenkin selkeyttää koordinoinnin sisällön osalta. Nykyinen yhteinen valvontaviranomainen on toimivaltainen tarkastelemaan yleissopimuksen tulkintaan ja soveltamiseen liittyviä ongelmia, tutkimaan riippumattoman valvonnan toteuttamisen tai käyttöoikeuden harjoittamisen yhteydessä mahdollisesti ilmeneviä ongelmia sekä laatimaan yhdenmukaistettuja ehdotuksia yhteisiksi ratkaisuiksi olemassa oleviin ongelmiin.

Uudet ehdotukset eivät saa johtaa siihen, että yhteisen valvonnan nykyistä soveltamisalaa heikennetään. Jos on selvää, että tietosuojaviranomaiset voivat käyttää SIS II:n osalta kaikkia niitä valvontaoikeuksia, jotka niille on annettu direktiivin nojalla, näiden viranomaisten yhteistyö voi kattaa laajoja osia SIS II:n valvonnasta, mukaan luettuna nykyisen yhteisen valvontaviranomaisen tehtävät, niin kuin ne on esitetty Schengenin yleissopimuksen 115 artiklassa.

Jotta tämä olisi täysin selvää, se olisi hyvä vahvistaa ehdotuksissa selväsanaisesti.

8. **TURVALLISUUS**

SIS II:n optimaalisen turvatason hallinta ja noudattaminen ovat perusedellytys tietokantaan tallennettujen henkilötietojen tarvittavan suojan varmistamiseksi. Tämän tyydyttävän turvatason toteuttamiseksi on otettava käyttöön asianmukaisia suojatoimenpiteitä järjestelmän infrastruktuuriin ja sitä käyttäviin henkilöihin liittyvien mahdollisten riskien varalta. Tätä kysymystä käsitellään ehdotuksen useissa kohdissa, mutta muotoilua on vielä parannettava.

Ehdotuksen 10 ja 13 artikloissa esitetään useita tietoturvaa koskevia toimenpiteitä ja erilaisia väärinkäyttötilanteita, jotka olisi estettävä. Tietosuojavaltuutettu on tyytyväinen siihen, että näihin artikloihin on sisällytetty säännöksiä turvatoimenpiteiden säännöllisestä (sisäisestä) valvonnasta.

Päätösehdotuksen 59 artiklan ja asetusehdotuksen 34 artiklan, joissa säädetään seurannasta ja arvioinnista, ei tulisi koskea pelkästään toiminnan tulosten, kustannustehokkuuden ja palvelujen laadun seurantaa ja arviointia vaan myös lakisääteisten vaatimusten noudattamista, erityisesti tietosuojan alalla. Tietosuojavaltuutettu suosittaa tästä syystä, että näiden artiklojen soveltamisalaa laajennetaan tietojen käsittelyn lainmukaisuuden valvontaan ja siitä raportointiin.

Lisäksi päätösehdotuksen 10 artiklan 1 kohdan f alakohtaa tai 18 artiklaa ja asetusehdotuksen 17 artiklaa olisi täydennettävä. Olisi lisättävä, että jäsenvaltioiden (ja Europolin ja Eurojustin) olisi varmistettava, että asianmukaisesti valtuutetulla henkilöstöllä, jolla on pääsy tietoihin, on tarkat käyttäjäprofiilit (jotka olisi pidettävä kansallisten valvontaviranomaisten saatavilla tarkastuksia varten). Näiden käyttäjäprofiilien lisäksi jäsenvaltioiden on laadittava täydellinen luettelo käyttäjistä ja pidettävä se jatkuvasti ajan tasalla. Sama koskee soveltuvin osin komissiota.

Näitä turvatoimenpiteitä täydennetään seurannalla ja organisatorisilla turvajärjestelyillä. Ehdotusten 14 artiklassa esitetään kaikkien tietojenkäsittelytapahtumien kirjaamisen edellytykset ja tarkoitus. Tietoja ei rekisteröidä vain tietosuojan valvomiseksi ja tietoturvan varmistamiseksi vaan myös 10 artiklan mukaista SIS II:n säännöllistä sisäistä valvontaa varten. Sisäistä valvontaa koskevat raportit auttavat osaltaan valvontaviranomaisia hoitamaan tehtävänsä tehokkaasti, määrittämään heikot kohdat sekä keskittymään niihin omissa valvontamenettelyissään.

Kuten aiemmin jo todettiin, järjestelmän liityntäpisteiden lisäämisen on oltava perusteltua, koska se automaattisesti lisää väärinkäytön riskiä. Ehdotusten 4 artiklan 1 kohdan b alakohdassa olisi vaadittava konkreettista osoitusta toisen liityntäpisteen tarpeesta.

Ehdotuksissa ei selitetä selvästi, miksi keskusjärjestelmästä tarvitaan kansalliset kopiot, mikä nostaa esiin vakavia yleiseen riskitasoon ja järjestelmän turvallisuuteen liittyviä huolenaiheita:

— Useat kopiot lisäävät väärinkäytön riskiä (erityisesti uusien tietomuotojen, kuten biometristen tietojen osalta).

— Kopioiden sisältämiä tietoja ei ole määritelty riittävän hyvin.

— 9 artiklan vaatimusten mukainen tarkkuus, laatu ja käytettävyys asettavat suuria teknisiä haasteita ja lisäävät kustannuksia käytettävissä olevan teknologian kehitystasosta riippuen.

— Kopioiden valvonta kansallisten viranomaisten toimesta edellyttää lisää henkilöstö- ja rahoitusresursseja, joita ei ehkä aina ole käytettävissä.

Asiaan liittyvä riskit huomioon ottaen tietosuojavaltuutettu ei ole vakuuttunut kansallisten kopioiden käytön tarpeellisuudesta eikä lisäarvosta (käytössä oleva teknologia huomioon ottaen). Tietosuojavaltuutettu suosittelee, että jäsenvaltioiden mahdollisuus käyttää kansallisia kopioita poistettaisiin.

Jos kansallisia kopioita kuitenkin aiotaan kehittää, tietosuojavaltuutettu muistuttaa, että niiden kansalliseen käyttöön on sovellettava tiukasti käyttötarkoituksen rajoittamisen periaatetta. Kansallisessa kopiossa ei myöskään saa tehdä hakuja eri tavalla kuin keskustietokannassa.

Henkilötietojen käsittelyn lainmukaisuus perustuu tietoturvan ja tietojen eheyden tiukkaan noudattamiseen. Tietosuojavaltuutettu valvoo tehokkaalla tavalla tietojen käsittelyä, jos valvonta ei rajoitu vain tietojen turvaamiseen vaan kattaa myös niiden eheyden käytettävissä olevien lokien analysoinnin avulla. Siksi on tarpeen lisätä ”tietojen eheys” 14 artiklan 6 kohtaan.

9. **KOMITEAMENETTELY**

Ehdotuksissa säädetään komiteamenettelyn noudattamisesta useissa sellaisissa tapauksissa, joissa on tehtävä SIS II:n täytäntöönpanoon tai hallitsemiseen liittyviä teknisiä päätöksiä. Kuten VIS-järjestelmää koskevassa lausunnossa todettiin samankaltaisista syistä, nämä päätökset vaikuttavat merkittävällä tavalla tarkoitusperiaatteen ja suhteellisuusperiaatteen asianmukaiseen soveltamiseen.

Tietosuojavaltuutettu suositteleekin, että tietosuojaan merkittävästi vaikuttavat päätökset, jotka koskevat esimerkiksi tietoihin pääsemistä ja tietojen tallentamista, lisätietojen vaihtamista, tietojen laatua ja ilmoitusten yhteensopivuutta, kansallisten kopioiden teknistä sääntöjenmukaisuutta, jne., olisi tehtävä asetuksen tai päätöksen muodossa, mieluiten yhteispäätösmenettelyä noudattaen. ([1])

([1]) Ks. myös Euroopan tietosuojavaltuutetun lausunto viisumitietojärjestelmästä (kohta 3.12) ja Euroopan tietosuojavaltuutetun lausunto ehdotuksesta direktiiviksi sellaisten tietojen säilyttämisestä, joita käsitellään yleisten sähköisten viestintäpalvelujen yhteydessä, annettu 26.9.2005 (kohta 60).

Kaikissa muissa tietosuojaan vaikuttavissa tapauksissa tietosuojavaltuutetulle olisi annettava mahdollisuus antaa lausunto komiteoiden tekemistä valinnoista.

Euroopan tietosuojavaltuutetun neuvoa-antava tehtävä olisi mainittava päätöksen 60 ja 61 artikloissa sekä asetuksen 35 artiklassa.

Ilmoitusten linkittämistä koskevien teknisten sääntöjen osalta (asetuksen 26 artikla ja päätöksen 46 artikla) on selitettävä eri komiteamenettelyjen tarve (neuvoa-antava menettely päätöksessä ja sääntelymenettely asetuksessa).

10. **YHTEENTOIMIVUUS**

Koska komissio ei ole vielä esittänyt tiedonantoa EU:n uusien järjestelmien yhteentoimivuudesta, on vaikea asianmukaisesti arvioida suunniteltujen mutta vielä määrittelemättömien yhteisvaikutusten lisäarvoa.

Tässä yhteydessä tietosuojavaltuutettu viittaa terrorismin torjunnasta annettuun neuvoston julkilausumaan (25.3.2004), jossa komissiota pyydetään esittämään ehdotuksia tietojärjestelmien (SIS, VIS ja Eurodac) yhteentoimivuuden ja yhteisvaikutuksen parantamiseksi. Tietosuojavaltuutettu haluaa myös mainita parhaillaan käytävät keskustelut siitä, mikä elin voisi huolehtia vastaisuudessa erilaisten laajojen järjestelmien hallinnoinnista (ks. myös tämän lausunnon 3.8. kohta).

Tietosuojavaltuutettu totesi jo viisumitietojärjestelmää koskevassa lausunnossaan, että yhteentoimivuus on keskeinen perusedellytys SIS II:n tapaisten laajamittaisten tietotekniikkajärjestelmien tehokkuudelle. Se auttaa vähentämään kokonaiskustannuksia johdonmukaisesti ja välttämään heterogeenisten elementtien aiheuttamaa redundanssia.

— Yhteentoimivuus voi myös osaltaan edistää korkean turvallisuustason säilyttämisen tavoitetta alueella, jolla jäsenvaltioiden välillä ei suoriteta sisäisiä rajatarkastuksia, sillä tällöin samaa menettelyä sovelletaan kaikkiin politiikan keskeisiin osiin. On kuitenkin tärkeää erottaa toisistaan kaksi yhteentoimivuuden tasoa:

  — Yhteentoimivuus EU:n jäsenvaltioiden välillä on erittäin toivottavaa; yhden jäsenvaltion viranomaisten lähettämien ilmoitusten tulee olla yhteentoimivia jonkin toisen jäsenvaltion viranomaisten lähettämien ilmoitusten kanssa.

  — Eri tarkoituksiin rakennettujen järjestelmien yhteentoimivuus tai yhteentoimivuus kolmansien maiden järjestelmien kanssa on paljon kyseenalaisempi asia.

Yksi järjestelmän tarkoituksen rajaamiseen tarkoitettuja suojatoimia, joilla estetään ns. *function creep* (tietojen käyttö muuhun kuin alkuperäiseen tarkoitukseen), on eri teknisten standardien käyttö. Lisäksi kahden eri järjestelmän vuorovaikutus olisi syytä dokumentoida perusteellisesti. Yhteentoimivuus ei saisi koskaan johtaa siihen, että viranomainen, jolla ei ole pääsyä järjestelmään eikä oikeutta käyttää joitakin tietoja, voi päästä järjestelmään toisen tietojärjestelmän kautta. Sikäli kun ehdotusten lukemisen perusteella voi tehdä luotettavia päätelmiä, vaikuttaa esimerkiksi siltä, että automaattinen sormenjälkien tunnistusjärjestelmä (AFIS) ei sisälly järjestelmään SIS II:n ensimmäisinä vuosina; ehdotuksissa mainitaan ainoastaan biometristen tietojen hakukoneet. Jos aiotaan käyttää EU:n muihin järjestelmiin sisältyviä sormenjälkien tunnistusjärjestelmiä, se olisi dokumentoitava selvästi ja otettava käyttöön tällaisten yhteisvaikutusten edellyttämät suojatoimet.

Tietosuojavaltuutettu haluaa jälleen kerran painottaa, että järjestelmien yhteentoimivuutta ei voi toteuttaa niin, että toimitaan vastoin käyttötarkoituksen rajoittamisen periaatetta, ja että kaikki tämänsuuntaiset ehdotukset tulisi toimittaa tietosuojavaltuutetulle.

11. **YHTEENVETO**

11.1 **Yleistä**

1. Euroopan tietosuojavaltuutettu pitää näiden ehdotusten useita kohtia myönteisinä, ja eräiltä osin ne merkitsevät parannusta nykytilanteeseen. Tietosuojavaltuutettu toteaa, että tietosuojasäännökset on yleisesti ottaen laadittu hyvin huolellisesti.

2. Euroopan tietosuojavaltuutettu painottaa, että olipa uusi järjestelmä kuinka monimutkainen tahansa, sen on

   — varmistettava tietosuojan korkea taso

   — oltava kansalaisten ja tietoja keskenään jakavien viranomaisten ennakoitavissa

   — oltava johdonmukainen, kun sitä sovelletaan eri yhteyksissä (ensimmäisessä ja kolmannessa pilarissa).

3. Koska SIS II -järjestelmään on lisätty uusia toimintoja, millä voi olla aiempaa enemmän vaikutuksia henkilöille, olisi suojatoimia tiukennettava. Näitä on kuvailtu lausunnossa. Erityisesti on huomattava seuraavaa:

— SIS II -järjestelmän käyttöoikeutta ei voida antaa uusille viranomaisille ilman erittäin hyviä perusteita. Käyttöoikeuksia tulisi rajoittaa mahdollisimman pitkälle sekä tietojen saatavuuden että tiedonsaantiin oikeutettujen henkilöiden osalta.

— Ilmoitusten linkittäminen ei saa koskaan epäsuorastikaan johtaa käyttöoikeuksien muutokseen.

— Vielä hyväksymätöntä lainsäädäntöä ei voida pitää pätevänä perusteena sille, että SIS II -järjestelmään viedään tietoja (ilmoitukset maahanpääsyn epäämiseksi).

— Ajoneuvojen rekisteritodistuksia myöntävien viranomaisten käyttöoikeutta koskevaa oikeusperustaa tulisi tarkastella uudelleen, koska se on pääasiallisesti rikosten torjuntaan liittyvä.

— Euroopan tietosuojavaltuutettu toteaa, että biometristen tietojen käyttäminen voi parantaa järjestelmän tehokkuutta ja auttaa henkilöllisyyden väärinkäytön kohteeksi joutuneita henkilöitä. Tämän lisäyksen vaikutuksia ei kuitenkaan ole tutkittu riittävästi ja näiden tietojen luotettavuutta on ehkä liioiteltu.

11.2 **Erityishuomioita**

1. Euroopan tietosuojavaltuutettu pitää myönteisenä komission kantaa siitä, että asetusta 45/2001 on sovellettava kaikkeen tietojen käsittelyyn, jota komissio suorittaa SIS II -järjestelmässä, koska näin varmistetaan osaltaan, että yksilöiden perusoikeuksien ja -vapauksien suojaamiseen tähtääviä sääntöjä noudatetaan henkilötietojen käsittelyssä johdonmukaisella tavalla ja yhdenmukaisesti.

2. Jotta käyttötarkoitus rajattaisiin tiukasti kansallisella tasolla, Euroopan tietosuojavaltuutettu suosittaa, että SIS II -ehdotuksiin (erityisesti asetusehdotuksen 21 artiklaan ja päätösehdotuksen artiklaan) sisällytetään samantyyppinen säännös kuin Schengenin yleissopimuksen 102 artiklan 4 kappaleessa, jossa rajoitetaan jäsenvaltioiden mahdollisuutta säätää tietojen käytöstä, josta ei ole mainintaa SIS II -teksteissä.

3. Kun jollekin viranomaiselle myönnetään SIS II -järjestelmän käyttöoikeus, olisi noudatettava tiukkoja ehtoja:

— Käyttöoikeuden olisi oltava SIS II:n yleisen tarkoituksen mukainen ja sopusoinnussa sen oikeusperustan kanssa.

— Tarve saada käyttöoikeus SIS II -järjestelmään on todistettava.

— Tietojen käyttötarkoitus on määriteltävä tarkasti ja rajattava.

— Käyttöoikeuden myöntämisedellytykset on määriteltävä ja rajattava hyvin. Erityisesti on laadittava ajantasainen luettelo henkilöistä, joilla on käyttöoikeus SIS II -järjestelmään, myös Europolissa ja Eurojustissa.

— Sitä, että nämä viranomaiset saavat SIS II:n käyttöoikeuden, ei saa käyttää perusteena tietojen syöttämiseksi järjestelmään ja säilyttämiseksi siellä, jos kyseiset tiedot eivät ole käyttökelpoisia sen ilmoituksen kannalta, jonka osia ne ovat.

— Tietojen säilyttämisaikaa ei tule pidentää, ellei se ole tarpeen sitä tarkoitusta varten, jonka vuoksi tiedot vietiin järjestelmään.

4. Europolin ja Eurojustin osalta Euroopan tietosuojavaltuutettu kehottaa komissiota rajaamaan ne tehtävät, joiden suorittamiseen käyttöoikeuden myöntäminen olisi perusteltua. Europolin ja Eurojustin oikeus käyttää tietoja olisi lisäksi rajattava tietoihin henkilöistä, joiden nimi on jo niiden tiedostoissa. On myös ehdotettu, että Europolille ja Eurojustille annettaisiin vain yksi liityntäpiste.

5. Maahanpääsyn epäämistä koskevien ilmoitusten osalta ne säännökset, jotka perustuvat lainsäädäntöön, jota ei ole vielä hyväksytty, olisi poistettava tai muotoiltava uudelleen — voimassa olevan lainsäädännön perusteella — niin, että henkilö voi saada tiedon siitä, mihin toimenpiteisiin viranomaiset tarkalleen ottaen voivat hänen suhteensa ryhtyä.

6. Tietojen säilyttämisaikoja on pidennetty, mutta tälle ei ole esitetty päteviä perusteita. Jos vakuuttavia perusteita ei löydy, ajat olisi palautettava nykyiselleen, erityisesti kun on kyse ilmoituksista tarkkailua tai erityistarkastuksia varten.

7. Komissio on vastuussa järjestelmän operatiivisesta hallinnoinnista. Sillä on myös tärkeä rooli järjestelmän kehittämisessä ja ylläpidossa, minkä vuoksi sitä voidaan pitää järjestelmän *sui generis* -valvojana. Tehtävään kuuluu paljon enemmän kuin tietojen käsittely, mutta toisaalta se on rajoitetumpi kuin tavanomainen valvontatehtävä, koska komissiolla ei ole SIS II -järjestelmässä käsiteltyjen tietojen käyttöoikeutta.

   Tämän tehtävän mukaisesti olisi kummankin ehdotuksen 12 artiklaan lisättävä, että komissio ehdottaa säännöllisesti tämän alan uuden huipputeknologian käyttöä, joka parantaa tietosuojan ja turvallisuuden tasoa.

8. Jäsenvaltioiden tehtävän osalta on selvitettävä, mitkä viranomaiset toimivat valvojina.

9. Rekisteröidyn informointi:

   — asetusehdotuksessa olisi lisättävä luetteloon joitain tietoja: tietojen säilyttämisaika, oikeus pyytää ilmoituksen tekemistä koskevan päätöksen tarkistusta tai oikeus valittaa siitä, mahdollisuus saada apua tietosuojaviranomaiselta sekä se, onko oikeussuojakeinoja käytettävissä.

     Lisäksi näiden tietojen antamisajankohdan osalta olisi lisättävä velvoite antaa tiedot ilmoituksesta päätöksessä, joka on ensisijaisesti ilmoituksen perusteena.

   — päätösehdotuksen 50 artiklaa (tiedonsaantioikeus) olisi muutettava niin, ettei rekisteröity joudu pyytämään tietoja niitä saadakseen.

10. Ehdotuksissa on asetettu määräajat tietojensaantia koskevaan pyyntöön vastaamiselle, mikä on hyvä asia. On selvennettävä, että jos myös kansallisessa lainsäädännössä asetetaan määräaikoja, että on sovellettava rekisteröidyn kannalta suotuisimpia määräaikoja.

    Lisäksi olisi hyvä säätää tietosuojaviranomaisten velvoitteesta tehdä aktiivisesti yhteistyötä tiedonsaantioikeuden myöntämisessä.

11. Oikeussuojakeinojen osalta Euroopan tietosuojavaltuutettu ehdottaa, että 30 artiklassa ja 52 artiklassa säädetty alueellinen rajoittaminen poistetaan.

12. Kansallisten tietosuojaviranomaisten toimivalta:

   — Asetuksessa on otettava huomioon, että kansalliset tietosuojaviranomaiset voivat käyttää SIS II:n osalta kaikkia niille direktiivin 95/46/EY 28 artiklan nojalla annettuja toimivaltuuksia; tämä olisi selvennettävä asetusehdotuksen tekstissä.

   — Päätösehdotuksessa valvontaviranomaisille olisi annettava samat toimivaltuudet kuin asetuksessa/direktiivissä.

13. Euroopan tietosuojavaltuutetun toimivalta: Euroopan tietosuojavaltuutetun pitäisi voida käyttää kaikkia asetuksen 45/2001 nojalla annettuja toimivaltuuksiaan ottaen kuitenkin huomioon komission rajalliset toimivaltuudet itse tietojen osalta.

14. Koordinoitu valvonta: ehdotuksissa on otettu huomioon tarve koordinoida eri viranomaisten valvontatoimet. Euroopan tietosuojavaltuutettu on tyytyväinen siihen, että ehdotukset sisältävät olennaisilta osin ne osatekijät, jotka ovat tarpeen yhteistyön mahdollistamiseksi valvonnasta vastaavien viranomaisten välillä kansallisella ja Euroopan tasolla. Näitä säännöksiä (asetusehdotuksen 31 artiklaa ja päätösehdotuksen 53 artiklaa) voitaisiin kuitenkin selkeyttää koordinoinnin sisällön osalta.

15. Ehdotuksen 10 ja 13 artiklassa on useita tietoturvaa koskevia toimenpiteitä; turvatoimenpiteiden säännöllisten (itse)valvontasäännösten sisällyttäminen on myönteistä.

   — Päätösehdotuksen 59 artiklan ja asetusehdotuksen 34 artiklan, joissa säädetään seurannasta ja arvioinnista, ei tulisi koskea pelkästään toiminnan tulosten, kustannustehokkuuden ja palvelujen laadun seurantaa ja arviointia vaan myös lakisääteisten vaatimusten noudattamista erityisesti tietosuojan alalla. Näitä säännöksiä tulisi tarkistaa tämän mukaisesti.

   — Lisäksi päätösehdotuksen 10 artiklan 1 kohdan f alakohtaa tai 18 artiklaa ja asetusehdotuksen 17 artiklaa olisi täydennettävä. Olisi lisättävä, että jäsenvaltioiden, Europolin ja Eurojustin olisi varmistettava, että käytettävissä on tarkat käyttäjäprofiilit (jotka olisi pidettävä kansallisten valvontaviranomaisten saatavilla tarkastuksia varten). Näiden käyttäjäprofiilien lisäksi jäsenvaltioiden on laadittava täydellinen luettelo käyttäjistä ja pidettävä se jatkuvasti ajan tasalla. Sama koskee komissiota.

   — Henkilötietojen käsittelyn lainmukaisuus perustuu siihen, että tietoturvaa ja tietojen eheyttä noudatetaan tiukasti. Euroopan tietosuojavaltuutetun olisi voitava valvoa paitsi tietojen turvaamista myös tietojen eheyttä käytettävissä olevien rekisterien avulla. Näin ollen 14 artiklan 6 kohtaan olisi lisättävä ”tietojen eheys”.

16. Kansallisten kopioiden käyttäminen voi lisätä riskejä huomattavasti. Euroopan tietosuojavaltuutettu ei ole vakuuttunut niiden käytön tarpeellisuudesta (käytössä oleva teknologia huomioon ottaen) eikä lisäarvosta. Euroopan tietosuojavaltuutettu suosittaa, että jäsenvaltioiden mahdollisuus kansallisten kopioiden käyttöön poistettaisiin tai että käyttöä ainakin rajoitettaisiin tiukasti. Jos kansallisia kopioita kuitenkin tehdään, on periaatteena oltava, että niiden käyttötarkoitus rajataan tarkoin. Kansallisessa kopiossa ei myöskään saa tehdä hakuja eri tavoin kuin keskustietokannassa.

17. Komiteamenettely: päätökset, joilla on huomattava vaikutus tietosuojaan, olisi tehtävä asetuksen tai päätöksen muodossa, mieluiten yhteispäätösmenettelyä noudattaen. Kun komiteamenettelyä tosiasiallisesti käytetään, Euroopan tietosuojavaltuutetun neuvoa-antava tehtävä olisi mainittava päätöksen 60 ja 61 artiklassa ja asetuksen 35 artiklassa.

18. Järjestelmien yhteentoimivuutta ei voi toteuttaa niin, että toimitaan vastoin käyttötarkoituksen rajoittamisen periaatetta. Kaikki tämänsuuntaiset ehdotukset tulisi toimittaa Euroopan tietosuojavaltuutetulle.

Tehty Brysselissä, 19. lokakuuta 2005

Peter HUSTINX

Euroopan tietosuojavaltuutettu