

**Euroopan tietosuojavaltuutetun lausunto komission neuvostolle ja Euroopan parlamentille
antamasta tiedonannosta "Vapauden, turvallisuuden ja oikeuden alue kansalaisia varten"**

(2009/C 276/02)

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,

ON ANTANUT SEURAAVAN LAUSUNNON:

I JOHDANTO

1. Komissio antoi 10 päivänä kesäkuuta 2009 neuvostolle ja Euroopan parlamentille tiedonannon vapauden, turvallisuuden ja oikeuden alueesta kansalaisia varten⁽¹⁾. Euroopan tietosuojavaltuutettu antaa tämän lausunnon asetuksen (EY) N:o 45/2001 41 artiklan mukaisesti.
2. Ennen tiedonannon antamista komissio tiedusteli epävirallisesti tietosuojavaltuutetun kantaa 19. toukokuuta 2009 päivätyllä kirjeellä. Tietosuojavaltuutettu vastasi tähän 20. toukokuuta 2009 lähettämällä epäviralliset huomautuksensa, joiden tarkoituksena oli tehdä parannuksia tiedonannon tekstiin. Lisäksi tietosuojavaltuutettu osallistui aktiivisesti poliisi- ja oikeusasioden työryhmän 14. tammikuuta 2009 päivätyyn vapauteen, turvallisuuteen ja oikeuteen perustuvaa aluetta koskevaa monivuotista ohjelmaa käsitelleen kirjeen laatimiseen⁽²⁾.
3. Tiedonannossa (kohta 1) korostetaan, että "EU:ssa tarvitaan uusi monivuotinen ohjelma, joka suuntautuu tähänastisten

⁽¹⁾ KOM(2009) 262 lopullinen ("tiedonanto").

⁽²⁾ Kirjettä ei ole julkaistu. Euroopan tietosuojavaltuutettujen konferenssi (European Conference of Data Protection Commissioners) perusti poliisi- ja oikeusasioden työryhmän valmistelemaan kantojaan lainvalvonnan alalla ja toimimaan puolestaan kiireellisissä tapauksissa.

edistysaskelten ja nykyisistä ongelmista saatujen kokemusten pohjalta kunnianhimoisesti tulevaisuuteen. Ohjelmassa olisi määriteltävä ensisijaiset tavoitteet seuraavaksi viideksi vuodeksi". Tämä monivuotinen ohjelma (joka tunnetaan jo "Tukholman ohjelmana") on jatkoa Tampereen ja Haagin ohjelmille, joissa annettiin voimakas poliittinen sysäys vapauden, turvallisuuden ja oikeuden alueelle.

4. Tiedonannon on tarkoitus toimia pohjana tälle uudelle monivuotiselle ohjelmalle. Tietosuojavaltuutettu toteaa tässä yhteydessä, että vaikka monivuotiset ohjelmat eivät sinänsä ole sitovia välineitä, niillä on huomattavaa vaikutusta toimielinten kyseisellä alla muodostamiin politiikkoihin, sillä ohjelma on lähtökohtana monille konkreettisille lainsäädäntö- ja muille toimille.
5. Itse tiedonantoa on tarkasteltava tästä näkökulmasta. Se on seuraava vaihe keskustelussa, joka enemmän tai vähemmän käynnistyi kahdesta neuvoston puheenjohtajan uusien ideoiden saamiseksi perustaman niin sanotun tulevaisuusryhmän kesäkuussa 2008 esittämästä raportista: "Vapaus, turvallisuus, yksityisyys – Euroopan sisäasiat avoimessa maailmassa"⁽³⁾ ja "Ratkaisuehdotuksia tulevaan EU:n oikeusalan ohjelmaan"⁽⁴⁾.

II LAUSUNNON PÄÄASIALLINEN SISÄLTÖ

6. Tässä lausunnossa ei ainoastaan reagoida tiedonantoon, vaan tietosuojavaltuutettu osallistuu sen muodossa vapauden, turvallisuuden ja oikeuden alueen tulevaisuutta koskevaan laajempaan keskusteluun, jonka on määrä johtaa uuteen strategiseen ohjelmaan (Tukholman ohjelma), kuten EU:n puheenjohtajavaltio Ruotsi on ilmoittanut⁽⁵⁾. Lausunnossa käsitellään myös joitakin Lissabonin sopimuksen mahdollisen voimaantumisen seurauksia.
7. Osassa III esitetään lausuntoon sisältyvät tärkeimmät näkökohdat, ja sen jälkeen osassa IV annetaan yleisarvio tiedonannosta.
8. Osassa V käsitellään kysymystä siitä, miten henkilötietojen vaihdon lisääntyessä voidaan vastata tarpeeseen kunnioittaa jatkossakin yksityisyyden ja henkilötietojen suojaa. Pääasiassa käsitellään tiedonannon kohtaa 2.3 henkilötietojen ja yksityisyyden suojasta ja yleisemmin uusia tietosuojan puitteiden parantamiseksi tarvittavia lainsäädäntö- ja muita toimia.

⁽³⁾ Neuvoston asiakirja N:o 11657/08. Jäljempänä 'raportti sisäasioista'.

⁽⁴⁾ Neuvoston asiakirja N:o 11549/08 ("raportti oikeusalaista").

⁽⁵⁾ Hallituksen EU-työohjelma, <http://www.regeringen.se>

9. Osassa VI käsitellään tarvetta ja mahdollisuuksia tietojen säilyttämiseen, niihin pääsyyn ja niiden vaihtoon lainvalvontavälineinä tai tiedonannon sanoin ilmaistuna siihen, että "EU suojaa kansalaisia". Tiedonannon kohta 4 sisältää useita tietovirtoja ja teknisiä välineitä koskevia tavoitteita, erityisesti kohdassa 4.1.2 (Tiedonhallinta), 4.1.3 (Tarvittavat tekniset välineet) ja 4.2.3.2 (Tietojärjestelmät). Eurooppalaisen tiedonhallintamallin kehittämistä (kohta 4.1.2) voidaan pitää tässä yhteydessä haastavimpana ehdotuksena. Tietosuojavaltuutetun lausunnossa analysoidaan tätä ehdotusta perusteellisesti.
10. Osassa VII käsitellään lyhyesti vapauden, turvallisuuden ja oikeuden alueiden sisällä erityistä tietosuojaan liittyvää aihetta, nimittäin oikeuspuojan saatavuutta ja sähköistä oikeutta.

III LAUSUNTOON SISÄLTÄVÄT NÄKÖKOHDAT

11. Tässä lausunnossa tarkastellaan tiedonantoa ennen kaikkea perusoikeuksien suojelun näkökulmasta ja yleisemmin vapauden, turvallisuuden ja oikeuden alueen tulevaisuuden kannalta sellaisena miksi se muodostuu uuden monivuotisen ohjelman puitteissa. Se perustuu lisäksi tietosuojavaltuutetun osallistumiseen EU:n politiikan kehittämiseen tällä alalla pääasiassa neuvoo-antavan tehtävänsä kautta. Tietosuojavaltuutettu on tähän mennessä antanut yli 30 lausuntoa ja kommenttia Haagin ohjelman perusteella tehdyistä aloitteista. Kaikki nämä ovat nähtävissä tietosuojavaltuutetun internet-sivustolla.
12. Arviossaan tiedonannosta tietosuojavaltuutettu ottaa huomioon erityisesti seuraavat neljä näkökohtaa, joilla on merkitystä vapauden, turvallisuuden ja oikeuden alueen kannalta. Kaikki nämä näkökohdat ovat keskeisiä myös komission tiedonannossa.
13. Ensimmäinen näkökohta on kansalaisia koskevien digitaalisten tietojen räjähdysmäinen kasvu tieto- ja viestintätekniikoiden kehittymisen tuloksena⁽⁶⁾. Yhteiskunta on muuttumassa yhä enemmän niin sanotuksi valvontayhteiskunnaksi, jossa kansalaisten kaikki toimet ja melkein kaikki liikkeet voivat tallentua digitaalisesti. Niin sanotut "esineiden internet" ja "älykäs toimintaympäristö" kehittyvät jo nopeasti älytunnisteiden (RFID-tunnisteiden) käytön avulla. Kehon digitaalisten piirteiden käyttö (biometriikka) lisääntyy jatkuvasti. Tämä johtaa entistä verkottuneempaan maailmaan,
- jossa yleisen turvallisuuden alan organisaatioilla on pääsy valtavaan määrään mahdollisesti käyttökelpoista tietoa, jolla voi olla välitöntä vaikutusta asianomaisten henkilöiden elämään.
14. Toinen näkökohta on kansainvälistyminen. Toisaalta Euroopan unionin ulkorajat eivät rajoita tiedonvaihtoa digitaalisena aikana ja toisaalta kansainvälistä yhteistyötä tarvitaan yhä enemmän monissa EU:n toimissa vapauden, turvallisuuden ja oikeuden alueella: terrorismin torjunta, poliisi- ja oikeudellinen yhteistyö, siviilioikeuden ala ja rajavalvonta ovat vain joitakin esimerkkejä tästä.
15. Kolmas näkökohta on tietojen käyttö lainvalvontatarkoituksiin: viimeaikaisten yhteiskuntaan kohdistuneiden uhkien johdosta, liittyivätpä ne terrorismiin tai eivät, on lisätty (vaadittu lisäämään) lainvalvontaviranomaisten mahdollisuuksia kerätä, tallentaa ja vaihtaa henkilötietoja. Monissa tapauksissa yksityisten osapuolten osallistuminen on aktiivista, mikä näkyy muun muassa tietojen säilyttämisestä koskevassa direktiivissä⁽⁷⁾ ja erilaisissa matkustajarekisteritietoihin liittyvissä välineissä⁽⁸⁾.
16. Neljäs näkökohta on vapaa liikkuvuus. Vapauden, turvallisuuden ja oikeuden alueen kehittäminen asteittain edellyttää, että sisärajojen ja vapaan liikkuvuuden mahdollisten esteiden poistamista alueella jatketaan. Tämän alan uusilla välineillä ei missään tapauksessa pitäisi luoda uusia esteitä. Vapaa liikkuvuus käsittää tässä yhteydessä toisaalta henkilöiden vapaan liikkuvuuden ja toisaalta (henkilö)tietojen vapaan liikkuvuuden.
17. Nämä neljä näkökohtaa ovat osoitus siitä, että yhteys, jossa tietoja käytetään, muuttuu nopeasti. Tällaisessa tilanteessa voimakkaalla mekanismilla on epäilemättä tärkeä merkitys kansalaisten perusoikeuksien suojelussa ja erityisesti yksityisyyden suojan ja tietosuojan takaamisessa. Näistä syistä tietosuojavaltuutettu on valinnut suojelutarpeen analyysinsä tärkeimmäksi näkökulmaksi, kuten edellä kohdassa 11 mainitaan.

⁽⁶⁾ Raportissa sisäasioista mainitaan tässä yhteydessä jopa "digitaalinen tsunami".

⁽⁷⁾ Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta, EUVL L 105, 13.4.2006, s. 54.

⁽⁸⁾ Ks. esim. Euroopan unionin ja Amerikan yhdysvaltojen välinen sopimus lentoyhtiöiden PNR- eli matkustajarekisteritietojen käsittelemisestä ja siirtämisestä Yhdysvaltojen turvallisuusministeriölle (DHS) (Vuoden 2007 PNR-sopimus), EUVL L 204, 4.8.2007, s. 18 ja ehdotus neuvoston puitepäättökseksi matkustajarekisterin (PNR) käytöstä lainvalvontatarkoituksiin, KOM(2007) 654 lopullinen.

IV YLEINEN ARVIOINTI

18. Tiedonannon ja Tukholman ohjelman tarkoituksena on määrittää EU:n suunnitelmat tuleviksi viideksi vuodeksi mahdollisesti vielä pidemmälle ulottuvine vaikutuksineen. Tietosuojavaltuutettu panee merkille, että tiedonanto on laadittu Lissabonin sopimuksen mahdollisen voimaantulon kannalta neutraalilla tavalla. Tietosuojavaltuutettu ymmärtää täysin, miksi komissio on valinnut tämän lähestymistavan, mutta pitää kuitenkin valitettavana, ettei tiedonannossa ole voitu hyödyntää kaikkia Lissabonin sopimuksen tarjoamia lisämahdollisuuksia. Lissabonin sopimuksen tarjoamiin mahdollisuuksiin kiinnitetään tässä lausunnossa enemmän huomiota.
19. Tiedonannon lähtökohtana ovat EU:n toiminnan tulokset vapauden, turvallisuuden ja oikeuden alueella. Tuloksia voidaan luonnehtia tapahtumalähtöisiksi painotuksen kohdistuessa toimenpiteisiin, jotka laajentavat lainvalvontaviranomaisten valtuuksia ja joilla puututaan kansalaisen yksityisyyteen. Näin on ainakin aloilla, joilla henkilötietoja käytetään ja vaihdetaan jatkuvasti ja joilla on sen takia tietosuojan kannalta keskeinen merkitys. Tulokset ovat tapahtumalähtöisiä, sillä ulkoiset tapahtumat, kuten syyskuun 11. päivän tapahtumat ja Madridin ja Lontoon pommi-iskut vauhdittivat lainsäädäntötoimintaa tuntuvasti. Esimerkiksi matkustajatietojen siirtäminen Yhdysvaltoihin voidaan nähdä seurauksena syyskuun 11. päivän tapahtumista⁽⁹⁾, ja Lontoon pommi-iskut johtivat direktiiviin 2006/24/EY tietojen säilyttämisestä⁽¹⁰⁾. Painopiste oli entistä enemmän yksityisyyteen puuttuvissa toimenpiteissä, sillä EU:n lainsäätävä keskittyi tietojen käyttöä ja vaihtoa helpottaviin toimenpiteisiin, kun taas toimenpiteitä henkilötietojen suojaamiseksi käsiteltiin vähemmän kiireellisinä. Tärkein hyväksytty suojatoimenpide on neuvoston puitepäätös 2008/977/YOS rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta⁽¹¹⁾. Päätös tehtiin sen jälkeen, kun sitä oli käsitelty neuvostossa kolme vuotta. Tuloksena oli neuvoston puitepäätös, joka ei ole täysin tyydyttävä (ks. kohta 29–30).
20. Viime vuosien kokemus on osoittanut, että ennen uusien välineiden hyväksymistä olisi pohdittava niiden seurauksia lainvalvontaviranomaisten ja Euroopan kansalaisten kannalta. Pohdinnassa olisi otettava huomioon niistä aiheutuvat haitat yksityisyydelle ja niiden tehokkuus lainvalvonnan kannalta, ensin uusia välineitä ehdotettaessa ja käsiteltäessä,
- mutta myös tekemällä määräaikaista tarkistuksia sen jälkeen, kun välineet on pantu täytäntöön. Tällainen pohdinta on tärkeää myös ennen kuin uudessa monivuotisessa ohjelmassa määritellään tärkeimmät lähitulevaisuudessa toteutettavat aloitteet.
21. Tietosuojavaltuutettu on tyytyväinen, että tiedonannossa tunnustetaan perusoikeuksien suoja, erityisesti henkilötietojen suoja, yhdeksi keskeisistä kysymyksistä vapauden, turvallisuuden ja oikeuden alueen tulevaisuuden kannalta. Tiedonannon kohdassa 2 EU:ta luonnehditaan yhteisiin arvoihin perustuvien perusoikeuksien suojelussa ainutlaatuiseksi alueeksi. On myös hyvä, että liittyminen Euroopan ihmisoikeussopimukseen mainitaan painopisteenä – jopa ensisijaisena kysymyksenä tiedonannossa. Sopimukseen liittyminen on merkittävä askel tasapainoisen ja johdonmukaisen perusoikeuksien suojelujärjestelmän varmistamisessa. Lisäksi tietosuojalle on tiedonannossa annettu näkyvä osa.
22. Tiedonannon kohdistaminen näihin kysymyksiin on osoitus voimakkaasta halusta varmistaa kansalaisten oikeuksien suojaaminen ja näin omaksua tasapainoisempi lähestymistapa. Hallitukset tarvitsevat asianmukaisia välineitä kansalaisten turvallisuuden takaamiseksi, mutta niiden on eurooppalaisessa yhteiskunnassamme kunnioitettava tinkimättä kansalaisten perusoikeuksia. Toiminta kansalaisten parhaaksi⁽¹²⁾ edellyttää, että Euroopan unioni huolehtii tämän tasapainon säilymisestä.
23. Tietosuojavaltuutettu katsoo, että tiedonannossa otetaan erittäin hyvin huomioon tämän tasapainon tarpeellisuus, myös tarve henkilötietojen suojaamiseen. Siinä tunnustetaan, että painotusta olisi muutettava. Tämä on tärkeää, koska vapauden, turvallisuuden ja oikeuden alueen politiikoilla ei pitäisi edistää siirtymistä vaiheittain kohti valvontayhteiskuntaa. Tietosuojavaltuutettu odottaa neuvoston omaksuvan saman lähestymistavan Tukholman ohjelmassa myös hyväksymällä jäljempänä kohdassa 25 esitetyt suuntaviivat.
24. Tämä on sitäkin tärkeämpää, koska vapauden, turvallisuuden ja oikeuden alue on alue, joka ”muokkaa kansalaisten elinolosuhteita, erityisesti heidän oman vastuunsa ja henkilökohtaisen turvallisuuden ja sosiaaliturvan yksityistä aluetta, joka on suojattu perusoikeuksilla”, kuten Saksan perustuslakituomioistuimen totesi 30. kesäkuuta 2009 Lissabonin sopimukseen liittyvässä tuomiossaan⁽¹³⁾.

⁽⁹⁾ Edellisessä alaviitteessä mainittu vuoden 2007 PNR-sopimus ja sen edeltäjät.

⁽¹⁰⁾ Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta, EUVL L 105, 13.4.2006, s. 54. Vaikka direktiivin oikeusperustana on EY:n perustamissopimuksen 95 artikla, se oli välitön vastaus Lontoon pommi-iskuihin.

⁽¹¹⁾ Neuvoston puitepäätös 2008/977/YOS, tehty 27 päivänä marraskuuta 2008, rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta, EUVL L 350, 30.12.2008, s. 60.

⁽¹²⁾ Ks. tiedonannon nimi.

⁽¹³⁾ Saksan liittotasavallan perustuslakituomioistuimen lehdistötiedote N:o 72/2009, 30. kesäkuuta 2009, kohta 2 c.

25. Tietosuojavaltuutettu korostaa, että tällä alueella:

- Tietojenvaihdon jäsenvaltioiden viranomaisten välillä ja tarvittaessa EU:n elinten tai tietokantojen välillä olisi tapahduttava käyttäen asianmukaisia ja tehokkaita mekanismeja, joissa kunnioitetaan tinkimättä kansalaisten perusoikeuksia ja joilla varmistetaan keskinäinen luottamus.
- Tämä edellyttää tietojen saatavuuden ja jäsenvaltioiden (ja EU:n) oikeusjärjestelmien keskinäisen tunnustamisen lisäksi tietojen suojaamista koskevien normien yhdenmukaistamista esimerkiksi, mutta ei yksinomaan, tietosuojaa koskevilla yhteisillä puitteilla.
- Näitä yhteisiä normeja ei pitäisi soveltaa pelkästään tilanteissa, joilla on rajatylittäviä ulottuvuuksia. Keskinäinen luottamus on mahdollista vain, kun normit ovat pysyviä ja niitä noudatetaan aina ilman vaaraa, että ne lakkaisivat olemasta voimassa heti, kun rajatylittävä ulottuvuus ei enää ole ilmeinen. Tämän lisäksi, erityisesti mitä tulee tietojen käyttöön, ero ”sisäisten” ja ”rajatylittävien” tietojen välillä ei ole käytännössä toimiva ⁽¹⁴⁾.

V TIETOSUOJAVÄLINEET

V.1 Kohti kattavaa tietosuojajärjestelmää

26. Tietosuojavaltuutettu hyväksyy strategisen lähestymistavan, jossa tietosuojalle annetaan tiedonannossa näkyvä sija. Monet aloitteet vapauden, turvallisuuden ja oikeuden alueella perustuvatkin henkilötietojen käyttöön, ja hyvällä tietosuojalla on niiden onnistumisen kannalta ratkaiseva merkitys. Yksityisyyden kunnioittaminen ja tietosuojat ovat paitsi lakisääteinen velvoite, joka tunnustetaan yhä laajemmin EU:n tasolla, myös Euroopan kansalaisten mielestä ratkaiseva kysymys, kuten Eurobarometrin tulokset osoittavat ⁽¹⁵⁾. Lisäksi henkilötietojen saannin rajoittamisella on myös ratkaiseva merkitys sen varmistamisessa, että lainvalvontaviranomaisten luottamus säilyy.
27. Tiedonannon kohdassa 2.3 todetaan, että tarvitaan laajalainen tietosuojajärjestelmä, joka kattaisi kaikki EU:n toimivaltaan kuuluvat alat ⁽¹⁶⁾. Tietosuojavaltuutettu antaa täy-

den tukensa tälle tavoitteelle Lissabonin sopimuksen voimaantulosta riippumatta. Hän toteaa myös, että tällainen järjestelmä ei välttämättä merkitse yhtä oikeudellista kehystä, jota sovellettaisiin kaikkeen tietojenkäsittelyyn. Nykyisten perussopimusten nojalla mahdollisuudet yhden kattavan oikeuskehyksen hyväksymiseen ovat rajoitetut pilarirakenteesta johtuen ja sen takia, että – ainakin ensimmäisessä pilarissa – EU:n toimielinten käsittelemien tietojen suojeleminen tapahtuu erilliseltä oikeusperustalta (EY:n perustamissopimuksen 286 artikla). Tietosuojavaltuutettu korostaa kuitenkin, että joitakin parannuksia voidaan toteuttaa hyödyntämällä kaikkia nykyisten perussopimusten tarjoamia mahdollisuuksia, kuten komissio on jo korostanut tiedonannossaan ”Haagin ohjelman täytäntöönpano: tulevat toimet” ⁽¹⁷⁾. Lissabonin sopimuksen voimaantulon jälkeen Euroopan unionin toiminnasta tehdyn sopimuksen 16 artikla muodostaa tarvittavan oikeusperustan yhdelle kattavalle oikeuskehykselle, jota sovellettaisiin kaikkeen tietojenkäsittelyyn.

28. Tietosuojavaltuutettu toteaa, että on joka tapauksessa tärkeää varmistaa tietosuojan oikeuskehyksen sisäinen johdonmukaisuus tarvittaessa yhdenmukaistamalla ja lujittamalla vapauden, turvallisuuden ja oikeuden alueella sovellettavia eri oikeudellisia välineitä.

Tilanne nykyisten perussopimusten ollessa voimassa

29. Ensimmäinen askel otettiin äskettäin tekemällä neuvoston puitepäätös 2008/977/YOS ⁽¹⁸⁾. Säädestä ei kuitenkaan voida pitää kattavana kehyksenä pääasiassa siksi, että sen säännöksiä ei sovelleta yleisesti. Niitä ei sovelleta sisäisiin tilanteisiin, joissa henkilötiedot ovat peräisin jäsenvaltiosta, joka niitä käyttää. Tällainen rajoitus vähentää väistämättä neuvoston puitepäätöksen lisäarvoa, elleivät jäsenvaltiot päättä sisällyttää sisäisiä tilanteita kansalliseen täytäntöönpanolainsäädäntöön, mikä ei ole todennäköistä.
30. Toinen syy, miksi tietosuojavaltuutettu katsoo, että pitkällä tähtäyksellä neuvoston puitepäätöksessä 2008/977/YOS ei ole riittävää vapauden, turvallisuuden ja oikeuden alueella sovellettavaa tietosuojakehystä, on se, että useat keskeiset säännökset eivät ole direktiivin 95/46/EY mukaisia. Nykyisten perussopimusten nojalla seuraava askel voisi olla neuvoston puitepäätöksen soveltamisalan laajentaminen ja sen yhdenmukaistaminen direktiivin 95/46/EY kanssa.
31. Kattavan tietosuojajärjestelmän toteuttamista voitaisiin vielä vauhdittaa laatimalla selkeä pitkän aikavälin visio. Siihen voisi kuulua yleinen johdonmukainen lähestymistapa tietojen keräämisen ja vaihdon – ja myös olemassa olevien

⁽¹⁴⁾ Tietosuojavaltuutettu on käsitellyt viimeksi mainittua näkökohtaa 19.12.2005 antamassaan lausunnossa ehdotuksesta neuvoston puitepäätökseksi rikosasioissa tehtävässä poliisiyhteistyössä ja rikosasioissa tehtävässä oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta (KOM(2005) 475 lopullinen), EUVL C 47, 25.2.2006, s. 27, 30–32 kohta.

⁽¹⁵⁾ Data Protection in the European Union — Citizens' perceptions — Analytical report, Flash Eurobarometer 225, tammik. 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

⁽¹⁶⁾ Ks. myös tiedonannon ensisijaiset suuntaukset.

⁽¹⁷⁾ KOM(2006) 331 lopullinen, 28. kesäkuuta 2006.

⁽¹⁸⁾ Ks. alaviite 11.

tietokantojen käytön – ja samalla tietosuojatakuiden määrittämiseksi. Tällaisella visiolla estettäisiin välineiden (ja siten henkilötietojen käsittelyn) tarpeeton päällekkäisyys. Sen pitäisi myös edistää EU:n politiikkojen johdonmukaisuutta alalla ja luottamusta siihen, miten viranomaiset käsittelevät kansalaisten henkilötietoja. Tietosuojavaltuutettu suosittelee neuvostolle, että se toteaisi selkeän pitkän aikavälin vision tarpeellisuuden Tukholman ohjelmassa.

32. Lisäksi tietosuojavaltuutettu suosittelee, että alalla jo hyväksytyt toimenpiteet, niiden konkreettinen täytäntöönpano ja niiden tehokkuus arvioidaan ja suhteutetaan. Tässä arvioinnissa olisi otettava asianmukaisesti huomioon haitat yksityisyyden kannalta ja tehokkuus lainvalvonnan kannalta. Jos arvioinnit osoittavat, että jotkut toimenpiteet eivät johda odotettuihin tuloksiin tai eivät ole oikeassa suhteessa haluttuun tarkoitukseen, olisi harkittava seuraavia toimenpiteitä:

— Ensiksi olisi muutettava tai peruutettava toimenpiteet siltä osin kuin ne eivät näytä olevan riittävästi perusteltuja konkreettisen lisäarvon tuottamiseksi lainvalvontaviranomaisille ja Euroopan kansalaisille.

— Toiseksi olisi arvioitava mahdollisuuksia parantaa olemassa olevien toimenpiteiden soveltamista.

— Vasta kolmanneksi olisi ehdotettava uusia lainsäädäntötoimenpiteitä, jos on todennäköistä, että niitä tarvitaan suunniteltuun tarkoitukseen. Uusia välineitä olisi hyväksyttävä vain, jos niillä on selkeää ja konkreettista lisäarvoa lainvalvontaviranomaisille ja Euroopan kansalaisille.

Tietosuojavaltuutettu suosittelee, että Tukholman ohjelmassa mainitaan olemassa olevien toimenpiteiden arviointijärjestelmä.

33. Lopuksi olisi myös tärkeää painottaa erityisesti olemassa olevien suojatoimenpiteiden parempaa täytäntöönpanoa tietosuojadirektiivin tehokkaampaa soveltamista koskevan työohjelman seurannasta annetun komission tiedonannon⁽¹⁹⁾ ja tietosuojavaltuutetun mainittua tiedonantoa koskevassa lausunnossa antamien ehdotusten mukaisesti⁽²⁰⁾. Valitettavasti komissiolla ei ole kolmannen pilarin puitteissa mahdollisuutta aloittaa rikkomismenettelyjä.

⁽¹⁹⁾ KOM(2007) 87 lopullinen, 7.3.2007.

⁽²⁰⁾ 25.7.2007 annettu lausunto, EUVL C 255, 27.10.2007, s. 1, erityisesti 30 kohta.

Tilanne Lissabonin sopimuksen ollessa voimassa

34. Lissabonin sopimus avaa mahdollisuudet todelliseen kattavaan tietosuojakehykseen. Euroopan unionin toiminnasta tehdyn sopimuksen 16 artiklan 2 kohdassa vaaditaan neuvostoa ja Euroopan parlamenttia vahvistamaan tietosuojasäännöt, jotka koskevat unionin toimielimiä, elimiä, toimistoja ja virastoja, jäsenvaltioita niiden toteuttaessa unionin lainsäädännön piiriin kuuluvia toimia ja yksityisiä osapuolia.

35. Tietosuojavaltuutetun käsityksen mukaan se, että tiedonannossa painotetaan kattavaa tietosuojajärjestelmää, johtuu komission pyrkimyksestä ehdottaa oikeuskehystä, jota sovellettaisiin kaikkeen tietojenkäsittelyyn. Hän antaa täyden tukensa tälle pyrkimykselle, joka lisää järjestelmän johdonmukaisuutta ja takaa oikeusvarmuuden ja näin parantaa suojaa. Sillä vältettäisiin tulevaisuudessa erityisesti vaikeudet, jotka syntyvät erosta pilarien välillä, kun yksityisellä sektorilla kaupallisiin tarkoituksiin kerättyä tietoa käytetään myöhemmin lainvalvontatarkoituksiin. Tämä pilarien välinen ero ei vastaa täysin todellisuutta, kuten matkustajarekisteriä⁽²¹⁾ ja tietojen säilyttämistä⁽²²⁾ koskevat yhteisöjen tuomioistuimen merkittävät tuomiot osoittavat.

36. Tietosuojavaltuutettu ehdottaa, että näitä perusteita kattavalle tietosuojajärjestelmälle korostettaisiin Tukholman ohjelmassa. Ne osoittavat, että tällainen järjestelmä ei ole vain suotava, vaan se on välttämätön, koska tietojen käyttöä koskevat käytännöt muuttuvat jatkuvasti. Hän suosittelee, että Tukholman ohjelman yhtenä painopisteenä olisi, että tarvitaan uusi lainsäädäntökehys, jolla muun muassa korvattaisiin neuvoston puitepäätös 2008/977/YOS.

37. Tietosuojavaltuutettu korostaa, että yleiseen oikeuskehykseen perustuvan kattavan tietosuojajärjestelmän käsite ei estä tietosuojaa koskevien lisäsääntöjen vahvistamista poliisi- ja oikeusalalla. Näissä lisäsääntöissä voitaisiin ottaa huomioon lainvalvonnan erityistarpeet, kuten Lissabonin sopimukseen liitetyssä julistuksessa 21 edellytetään⁽²³⁾.

V.2 Tietosuojan periaatteiden ilmaiseminen uudelleen

38. Tiedonannossa todetaan tekniset muutokset, jotka muuttavat viestintää yksilöiden ja julkisten sekä yksityisten organisaatioiden välillä. Komissio katsoo, että tämän takia on ilmaistava uudelleen joitakin tietosuojan peruseriaatteita.

⁽²¹⁾ Yhteisöjen tuomioistuimen tuomio 30. toukokuuta 2006, Euroopan parlamentti v. Euroopan unionin neuvosto (C-317/04) ja Euroopan yhteisöjen komissio (C-318/04), yhdistetyt asiat C-317/04 ja C-318/04, Kok. 2006, s. I-4721.

⁽²²⁾ Yhteisöjen tuomioistuimen tuomio 10. helmikuuta 2009, Irlanti v. Euroopan parlamentti ja neuvosto, asia C-301/06, ei vielä julkaistu.

⁽²³⁾ Ks. julistus 21 henkilötietojen suojasta rikosoikeuden alalla tehtävän oikeudellisen yhteistyön ja poliisiyhteistyön aloilla, liitetty Lissabonin sopimuksen hyväksyneen hallitustenvälisen konferenssin päätöksiin, EUVL C 115, 9.5.2008, s. 345.

39. Tietosuojavaltuutettu on tyytyväinen näihin tiedonannossa esitettyihin suunnitelmiin. Näiden periaatteiden tehokkuuden arviointi teknologisten muutosten näkökulmasta on erittäin hyödyllistä. Ensinnäkin on tärkeää todeta, että tietosuojaperiaatteiden uudelleenilmaisemisen ja vahvistamisen ei välttämättä tarvitse aina liittyä suoraan tekniikan kehitykseen. Sitä voidaan tarvita myös muista, edellä osassa III mainituista syistä, joita ovat esimerkiksi kansainvälistyminen, tietojen kasvava käyttö lainvalvonnassa ja vapaa liikkuvuus.
40. Lisäksi tietosuojavaltuutettu katsoo, että tämä arviointi voidaan sisällyttää julkiseen kuulemiseen, josta komissio ilmoitti aiheesta "Personal data – more use, more protection?" 19. ja 20. toukokuuta 2009 järjestetyssä konferenssissa. Tästä julkisesta kuulemisesta voisi olla huomattavaa hyötyä⁽²⁴⁾. Tietosuojavaltuutettu ehdottaa, että neuvosto korostaisi Tukholman ohjelmassa ja komissio kuulemisesta koskevista julkisista lausunnoistaan yhteyttä tiedonannon kohdan 2.3 suunnitelmien ja tietosuojan tulevaisuutta koskevan kuulemisen välillä.
41. Esimerkkinä siitä, mitä tällaiseen arviointiin voisi kuulua, todetaan seuraavaa:
- Vapauden, turvallisuuden ja oikeuden alueella käsiteltävät henkilötiedot, kuten rikostuomioihin liittyvät tiedot, poliisitiedot ja biometriset tiedot, esimerkiksi sormenjäljet ja DNA-tunnisteet, saattavat olla erityisen arkaluonteisia.
 - Niiden käsittelystä voi aiheutua kielteisiä seurauksia rekisteröidyille erityisesti, kun otetaan huomioon lainvalvontaviranomaisten käytettävissä olevat pakkokeinot. Lisäksi tietojen seuranta ja analysointi on lisääntyvässä määrin automatisoitu, ja se tapahtuu usein ilman inhimillistä panosta. Tekniikka on tehnyt mahdolliseksi henkilötietokantojen käytön yleisiin hakutoimintoihin (tietojen louhinta, profilointi, jne.). Lakisäateiset velvoitteet, joihin tietojenkäsittely perustuu, olisi asetettava selkeästi.
 - Tietosuojalainsäädännön kulmakiviä on, että henkilötiedot on kerättävä määriteltävä tarkoitusta varten eikä niitä saa käyttää tavalla, joka ei vastaa tätä tarkoitusta. Käyttö, joka ei vastaa tiettyä tarkoitusta, olisi sallittava vain siinä tapauksessa, että siitä on säädetty laissa ja se on välttämätöntä erityisen yleisen edun ajamiseksi, kuten Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohdassa mainitut edut.
 - Sillä, että on noudatettava käyttötarkoituksen rajoittamisen periaatetta, saattaa olla vaikutusta tietojen käyttöön nykyisiin suuntauksiin. Lainvalvonnassa käytetään tietoja, joita yksityiset yritykset ovat keränneet kaupallisiin tarkoituksiin televiestintä-, kuljetus- ja rahoitusaloilla. Lisäksi esimerkiksi maahanmuuton ja rajavalvonnan alalla on perustettu laajamittaisia tietojärjestelmiä. Myös yhteenliittäminen ja pääsy tietokantoihin on sallittua, mikä laajentaa tarkoituksia, joihin henkilötiedot on alunperin kerätty. Näitä nykyisiä suuntauksia olisi tarkasteltava ja tehtävä tarvittaessa mahdollisia parannuksia ja/tai lisättävä suojatoimia.
- Tiedonannossa mainittujen tietosuojan periaatteiden lisäksi arvioinnissa olisi kiinnitettävä huomiota käsittelyn avoimuuteen niin, että rekisteröidyllä on mahdollisuus käyttää oikeuksiaan. Avoimuus on erityisen vaikea kysymys lainvalvonnan alalla varsinkin, koska avoimuutta olisi punnittava tutkinnan vaarantumisen kannalta.
- Kolmansien maiden kanssa harjoitettavaan tiedonvaihtoon olisi löydettävä ratkaisuja.
42. Arvioinnissa olisi lisäksi kiinnitettävä huomiota mahdollisuuksiin tehostaa tietosuojaperiaatteiden soveltamista. Tässä yhteydessä voisi olla hyödyllistä keskittyä välineisiin, joilla voidaan lisätä rekisterinpitäjien velvollisuuksia. Näillä välineillä on mahdollistettava rekisterinpitäjien täydellinen vastuuvollisuus tiedonhallinnasta. "Tietojen hallinnointi" on hyödyllinen käsite tässä yhteydessä. Se kattaa kaikki oikeudelliset, tekniset ja organisatoriset keinot, joilla organisaatio varmistaa täyden vastuun ottamisen tavasta, jolla tietoja käsitellään, kuten suunnittelu ja valvonta, tarkoituksenmukaisen teknologian käyttö, henkilöstön riittävä koulutus, sääntöjen noudattamista koskevat tarkastukset jne.

V.3 Yksityisyyden huomioon ottavat teknologiat

43. Tietosuojavaltuutettu on tyytyväinen, että tiedonannon kohdassa 2.3 mainitaan yksityisyyden huomioon ottamista koskeva sertifiointi. Sen lisäksi voitaisiin mainita "sisäänrakennettu yksityisyyden suoja" ja se, että olisi määriteltävä "parhaat käytettävissä olevat tekniikat", jotka vastaavat EU:n tietosuojakehystä.
44. Tietosuojavaltuutettu katsoo, että "sisäänrakennettu yksityisyyden suoja" ja yksityisyyden huomioon ottavat teknologiat voisivat olla hyödyllisiä välineitä tietosuojan parantamiseksi ja myös tietojen käytön tehostamiseksi. Tietosuojavaltuutettu ehdottaa kahta, ei välttämättä toisiaan poissulkevaa etenemistapaa:
- Tietojärjestelmien rakentajille ja käyttäjille valinnaisena tarjottava yksityisyyden ja tietosuojan sertifiointijärjestelmä⁽²⁵⁾, jota voitaisiin tukea tai olla tukematta EU:n rahoituksella tai EU:n lainsäädännöllä.

⁽²⁴⁾ 29 artiklan mukainen tietosuojatyöryhmä, johon tietosuojavaltuutettu osallistuu, on päättänyt työskennellä tiivistä antaakseen oman panoksensa julkiseen kuulemiseen.

⁽²⁵⁾ Esimerkki tällaisesta järjestelmästä on eurooppalainen yksityisyyden suoja koskeva tunnus (European Privacy Seal — EuroPriSe).

— Tietojärjestelmien rakentajille ja käyttäjille asetettu velvoite käyttää järjestelmiä, jotka ovat sisäänrakennetun yksityisyyden suojan periaatteen mukaisia. Tämä saattaisi edellyttää nykyisen tietosuojalainsäädännön soveltamisalan laajentamista siten, että järjestelmien rakentajat velvoitettaisiin vastaamaan kehittämistään tietojärjestelmistä ⁽²⁶⁾.

Tietosuojavaltuutettu ehdottaa, että nämä mahdolliset etenemistavat mainitaan Tukholman ohjelmassa.

V.4 Ulkoiset näkökohdat

45. Toinen tiedonannossa mainittu aihe on kansainvälisten tietosuojanormien kehittäminen ja edistäminen. Tällä hetkellä on meneillään useita toimia (esimerkiksi tietosuojavaltuutettujen kansainvälisen konferenssin yhteydessä) sellaisten toteuttamiskelpoisten normien laatimiseksi, joita voitaisiin soveltaa yleisesti. Lähtötulevaisuudessa nämä toimet saattavat johtaa kansainväliseen sopimukseen. Tietosuojavaltuutettu ehdottaa, että Tukholman ohjelmassa tuetaan näitä toimia.
46. Tiedonannossa mainitaan myös kahdenvälisen sopimusten tekeminen Yhdysvaltojen kanssa jo yhdessä saavutetun edistyksen pohjalta. Tietosuojavaltuutettu on yhtä mieltä siitä, että tietojen siirrolle kolmansiin maihin tarvitaan selkeää oikeuskehystä, ja on näin ollen tyytyväinen EU:n ja Yhdysvaltain viranomaisten korkean tason kontaktiryhmässä tekemään mahdollista transatlanttista tietosuojavälinettä koskevaan työhön, mutta toivoo lisää selkeyttä ja huomion kiinnittämistä erityisiin kysymyksiin ⁽²⁷⁾. Tästä näkökulmasta on myös mielenkiintoista panna merkille sisäasioita koskevassa raportissa esitetyt ajatukset euro-atlanttisesta yhteistyöalueesta vapauden, turvallisuuden ja oikeuden alalla. Raportin mukaan EU:n olisi päätettävä siitä vuoteen 2014 mennessä. Tällainen yhteistyöalue ei ole mahdollinen ilman kunnollisia takuita tietosuojasta.
47. Tietosuojavaltuutettu katsoo, että Euroopan tietosuojanormien, jotka perustuvat Euroopan neuvoston yleissopimukseen 108 yksilöiden suojelusta henkilö tietojen suojaamisesta tietojenkäsittelyssä ⁽²⁸⁾ sekä Euroopan yhteisöjen tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oike-

uskäytäntöön, olisi määrättävä tietosuojasta ja tietojenvaihdosta Yhdysvaltojen kanssa tehtävän yleisen sopimuksen suojelutaso. Tällainen yleinen sopimus voisi olla perustana henkilötietojen vaihtoa koskeville erityisjärjestelyille. Tämä on sitäkin tärkeämpää, kun otetaan huomioon tiedonannon kohdassa 4.2.1 ilmaistu pyrkimys, että Euroopan unionin olisi tehtävä poliisiyhteistyösopimuksia aina, kun se tarpeen.

48. Tietosuojavaltuutettu ymmärtää täysin, että kansainvälistä yhteistyötä on lisättävä, joissakin tapauksissa myös sellaisten maiden kanssa, jotka eivät suojaa perusoikeuksia. On kuitenkin ⁽²⁹⁾ ratkaisevan tärkeää ottaa huomioon, että tämä kansainvälinen yhteistyö johtaa todennäköisesti siihen, että tietojenkeruu ja kansainvälinen tietojen siirto lisääntyy huomattavasti. Sen vuoksi on tärkeää, että asianmukaisen ja laillisen käsittelyn periaatteita – sekä asianmukaisen käsittelyn periaatteita yleensä – sovelletaan henkilötietojen keräämiseen ja siirtoon unionin rajojen yli ja että henkilötietoja siirretään kolmansiin maihin tai kansainvälisille organisaatioille ainoastaan, jos kyseiset kolmannet osapuolet takaavat suojan riittävän tason tai muut asianmukaiset suojatoimet.
49. Lopuksi tietosuojavaltuutettu suosittelee, että Tukholman ohjelmassa korostetaan Yhdysvaltojen ja muiden kolmansien maiden kanssa tietosuojasta ja tietojenvaihdosta tehtävien sellaisten yleisten sopimusten merkitystä, jotka perustuvat EU:n alueella taattuun suojan tasoon. Laajemmin tietosuojavaltuutettu korostaa, että suhteissa kolmansiin maihin ja kansainväliin järjestöihin on tärkeää edistää aktiivisesti perusoikeuksien kunnioitusta ja erityisesti tietosuojaa ⁽³⁰⁾. Lisäksi Tukholman ohjelmassa voitaisiin mainita yleisenä huomiona, että henkilötietojen vaihto kolmansien maiden kanssa edellyttää suojan riittävää tasoa tai muita asianmukaisia suojatoimia kyseisissä kolmansissa maissa.

VI TIETOJEN KÄYTTÖ

VI.1 Kohti eurooppalaista tiedonhallintamallia

50. Tietojenvaihdon parantaminen on Euroopan unionin keskeinen poliittinen tavoite vapauden, turvallisuuden ja oikeuden alueella. Tiedonannon kohdassa 4.1.2 korostetaan, että Euroopan unionin turvallisuus riippuu tehokkaista

⁽²⁶⁾ Tietosuojalainsäädäntö kattaa tietojen käyttäjät samoin kuin rekisterinpitäjät tai tietojen käsittelijät.

⁽²⁷⁾ Ks. tietosuojavaltuutetun 11. marraskuuta 2008 antama lausunto tietojenvaihtoa, yksityisyyden suojaa ja henkilö tietojen suojaamista käsittelevän EU:n ja Yhdysvaltojen korkean tason kontaktiryhmän loppuraportista, EUVL C 128, 6.6.2009, s. 1.

⁽²⁸⁾ Euroopan neuvoston sopimussarja N:o 108, 28.1.1981.

⁽²⁹⁾ Ks. tietosuojavaltuutetun 28. marraskuuta 2005 päivätty kirje, joka koskee komission tiedonantoa vapauden, turvallisuuden ja oikeuden alueen ulkoisesta ulottuvuudesta. Kirje on nähtävissä tietosuojavaltuutetun verkkosivuilla.

⁽³⁰⁾ Äskettäinen oikeuskäytäntö terroristien luetteloista on osoitus siitä, että takuita tarvitaan – myös suhteissa Yhdistyneisiin Kansakuntiin – sen varmistamiseksi, että terrorismin vastaiset toimet ovat perusoikeuksia koskevien EU:n normien mukaisia (yhdistetyissä asioissa C-402/05 P ja C-415/05 P, Kadi ja Al Barakaat Foundation v. neuvosto, 3. syyskuuta 2008 annettu tuomio, ei vielä julkaistu).

- kansallisten viranomaisten ja muiden eurooppalaisten toimijoiden välisestä tiedonvaihtojärjestelmästä. Euroopan poliisivuimien, Euroopan rikosoikeusjärjestelmän ja Euroopan rajavalvonnan puuttuessa on luonnollista, että tietojenvaihtoa korostetaan. Tietoihin liittyvät toimenpiteet ovat tämän takia Euroopan unionin keskeinen keino auttaa jäsenvaltioiden viranomaisia käsittelemään rajatylittävää rikollisuutta ja suojelemaan ulkorajoja tehokkaasti. Ne eivät kuitenkaan pelkää lisää kansalaisten turvallisuutta, vaan myös heidän vapauttaan – henkilöiden vapaa liikkuvuus mainittiin edellä yhtenä tämän lausunnon näkökohtana – ja oikeutta.
51. Juuri näistä syistä Haagin ohjelmassa otettiin käyttöön saatavuusperiaate. Se tarkoittaa, että rikosten torjunnassa tarvittavien tietojen olisi voitava ylittää EU:n sisäraajat esteettömästi. Viimeaikaiset kokemukset osoittavat, että tätä periaatetta on ollut vaikeaa panna täytäntöön lainsäädäntötoimin. Neuvosto ei hyväksynyt komission 12 päivänä lokakuuta 2005 esittämää ehdotusta neuvoston puitepäätökseksi saatavuusperiaatteen mukaisesta tietojenvaihdosta⁽³¹⁾. Jäsenvaltiot eivät olleet valmiita hyväksymään täydellisestä saatavuusperiaatteesta aiheutuvia seurauksia. Sen sijaan hyväksyttiin rajoitetumpia välineitä⁽³²⁾, kuten rajatylittävän yhteistyön tehostamisesta erityisesti terrorismin ja rajatylittävän rikollisuuden torjumiseksi 23. kesäkuuta 2008 tehty neuvoston päätös 2008/615/YOS (Prüm-päätös)⁽³³⁾.
52. Saatavuusperiaate oli Haagin ohjelmassa keskeinen, mutta komissio näyttää nyt omaksuneen vaatimattomamman lähestymistavan. Sen tarkoituksena on edistää jäsenvaltioiden viranomaisten välistä tietojenvaihtoa ottamalla käyttöön eurooppalainen tiedonhallintamalli. EU:n puheenjohtajavaltio Ruotsi on samoilla linjoilla⁽³⁴⁾. Se aikoo antaa ehdotuksen tiedonvaihtostrategiasta. Neuvosto on jo aloittanut työn tämän kunnianhimoisen hankkeen, Euroopan unionin tiedonhallintastrategian laatimiseksi. Strategia liittyy kiinteästi eurooppalaiseen tiedonhallintamalliin. Tietosuojavaltuutettu panee tämän kehityksen mielenkiinnolla merkille ja korostaa, että hankkeissa olisi kiinnitettävä huomiota tietosuojaan liittyviin seikkoihin.
- Eurooppalainen tiedonhallintamalli ja tietosuoja*
53. Aluksi on korostettava, että vapauden, turvallisuuden ja oikeuden alueen tulevaisuus ei saisi määräytyä teknologian lähtökohdista, eli uusien tekniikoiden tarjoamia lähes rajattomia mahdollisuuksia olisi aina tarkasteltava suhteessa asianmukaisiin tietosuojaperiaatteisiin ja käytettävä vain silloin, kun ne ovat näiden periaatteiden mukaisia.
54. Tietosuojavaltuutettu toteaa, että tiedonannossa ei esitetä tiedonhallintamallia pelkästään teknisenä mallina, vaan myös vahvana strategisena analyysivalmiutena ja operatiivisten tietojen tehokkaampana keräämisellä ja käsittelyllä. Siinä tunnustetaan myös, että toimintapolitiittiset näkökohdat, kuten tietojen keräämistä, jakamista ja käsittelyä koskevat kriteerit, olisi otettava huomioon ja samalla noudatettava tietosuojaperiaatteita.
55. Sekä tietotekniikalla että oikeudellisilla edellytyksillä on, ja tulee olemaan, keskeinen merkitys. Tietosuojavaltuutettu on tyytyväinen tiedonantoon, jossa lähdetään siitä, että eurooppalaista tiedonhallintamallia ei voi perustaa teknisille näkökohdille. On olennaisen tärkeää, että tietoja kerätään, jaetaan ja käsitellään ainoastaan konkreettisten turvallisuustarpeiden perusteella ja ottaen huomioon tietosuojaperiaatteet. Tietosuojavaltuutettu on myös täysin samaa mieltä siitä, että olisi määriteltävä seurantamekanismi sen arvioimiseksi, miten tietojenvaihto toimii. Hän ehdottaa, että neuvosto kehrittelee Tukholman ohjelmassa edelleen näitä näkökohtia.
56. Tietosuojavaltuutettu korostaa tässä yhteydessä, että tietosuoja, jonka tarkoituksena on kansalaisten suojeleminen, ei pitäisi nähdä esteenä tehokkaalle tiedonhallinnalle. Se tarjoaa tärkeitä välineitä tiedon tallentamisen, saatavuuden ja vaihdon parantamiseksi. Rekisteröidyn oikeus saada tietoa siitä, mitä häntä koskevia tietoja käsitellään, ja oikeus korjata virheelliset tiedot, voi myös lisätä tietojen luotettavuutta tiedonhallintajärjestelmissä.
57. Tietosuojalainsäädännöllä on pääasiassa seuraavia vaikutuksia: jos tietoja tarvitaan erityiseen oikeutettuun tarkoitukseen, niitä voidaan käyttää; jos niitä ei tarvita hyvin määriteltävään tarkoitukseen, henkilötietoja ei pitäisi käyttää. Ensimmäisessä tapauksessa saatetaan tarvita lisätoimenpiteitä asianmukaisten suojatoimenpiteiden varmistamiseksi.
58. Tietosuojavaltuutettu suhtautuu kuitenkin kriittisesti siihen, miten pitkälle tiedonannossa todetaan ”tulevien tarpeiden selvittämisen” olevan osa tiedonhallintamallia. Hän korostaa, että käyttötarkoituksen rajoittamisen periaatteen olisi tulevaisuudessakin oltava johtavana periaatteena tietojärjestelmiä perustettaessa⁽³⁵⁾. Se on yksi tietosuojajärjestelmän kansalaiselle antamista olennaisista takuista: hänen on voitava tietää edeltä käsin, mitä tarkoitusta varten häneen liittyviä tietoja kerätään, ja että niitä käytetään vain siihen tarkoitukseen, erityisesti tulevaisuudessa. Tämä takuu on myös kirjattu Euroopan unionin perusoikeuskirjan 8 artiklaan. Käyttötarkoituksen rajoittamisen periaatteesta on poikkeuksia, erityisesti vapauden, turvallisuuden ja oikeuden alueella, mutta näiden poikkeusten ei pitäisi olla määräviä järjestelmää luotaessa.

⁽³¹⁾ KOM(2005) 490 lopullinen.

⁽³²⁾ Saatavuusperiaatteen näkökulmasta Prüm-päätös sisältää pitkälle meneviä säännöksiä biometristen tietojen (DNA ja sormenjäljet) käytöstä.

⁽³³⁾ EUVL L 210, 6.8.2008, s. 1.

⁽³⁴⁾ Ks. alaviitteessä 5 mainittu hallituksen EU-työohjelma, s. 23.

⁽³⁵⁾ Ks. myös kohta 41 edellä.

Oikean arkkitehtuurin valitseminen

59. Oikean arkkitehtuurin valitseminen tietojenvaihtoa varten on kaiken lähtökohta. Kunnollisten tietojärjestelmäarkkitehtuurien merkitys tunnustetaan tiedonannossa (kohta 4.1.3), mutta valitettavasti vain yhteentoimivuuteen liittyen.
60. Tietosuojavaltuutettu korostaa toista näkökohtaa: tietosuojavaltuutuksen olisi eurooppalaisessa tiedonhallintamallissa oltava erottamaton osa järjestelmän kehittämistä eikä niitä saisi nähdä vain tarvittavana edellytyksenä sille, että järjestelmä on lain mukainen ⁽³⁶⁾. Olisi käytettävä ”sisäänrakennetun yksityisyyden suojan” ja ”parhaiden käytettävissä olevien tekniikoiden” käsitteitä ⁽³⁷⁾, jotka esiteltiin edellä kohdassa 43. Eurooppalaisen tiedonhallintamallin olisi perustuttava näihin käsitteisiin. Tämä merkitsee käytännössä, että yleisen turvallisuuden tarkoituksiin suunnitellut tietojärjestelmät olisi aina suunniteltava ”sisäänrakennetun yksityisyyden suojan” periaatteen mukaisesti. Tietosuojavaltuutettu suosittelee, että neuvosto sisällyttäisi nämä seikat Tukholman ohjelmaan.

Järjestelmien yhteentoimivuus

61. Tietosuojavaltuutettu korostaa, että yhteentoimivuus ei ole pelkästään tekninen kysymys, vaan sillä on merkitystä kansalaisten suojelun, erityisesti tietosuojan kannalta. Tietosuojan näkökulmasta järjestelmien yhteensopivuudesta, jos se on hyvin toteutettu, on selvää etua, koska sillä vältetään tietojen päällekkäinen säilyttäminen. On kuitenkin myös ilmeistä, että tietojen saatavuuden ja vaihdon tekeminen teknisesti mahdolliseksi johtaa monissa tapauksessa voimakkaaseen pyrkimykseen todella myös saada tai vaihtaa näitä tietoja. Toisin sanoen yhteentoimivuudessa on se erityinen vaara, että eri tarkoituksiin käytettävät tietokannat liitetään yhteen ⁽³⁸⁾. Tämä voi vaikuttaa tietokantojen taroitusta koskeviin tiukkoihin rajoituksiin.
62. Lyhyesti sanottuna pelkästään se, että on teknisesti mahdollista vaihtaa digitaalisia tietoja yhteentoimivien tietokantojen välillä tai yhdistää tietokantoja, ei anna oikeutta poiketa käyttötarkoituksen rajoittamisen periaatteesta. Yhteentoimivuuden olisi käytännössä perustuttava selkeisiin ja harkit-

tuihin toimintapoliittisiin valintoihin. Tietosuojavaltuutettu ehdottaa, että käsitettä tarkennetaan Tukholman ohjelmassa.

VI.2 Muihin tarkoituksiin kerättyjen tietojen käyttö

63. Tiedonannossa ei suoranaisesti käsitellä viime vuosien tärkeimpiä suuntauksia, kuten yksityissektorilla kaupallisiin tarkoituksiin kerättyjen tietojen käyttöä lainvalvontatarkoituksiin. Tämä suuntaus ei liity sähköisen viestinnän liikennetietoihin ja (tiettyihin) kolmansiin maihin lentävien henkilöiden matkustajatietoihin ⁽³⁹⁾, vaan se koskee myös rahoitusala. Rahoitusjärjestelmän käytön estämisestä rahanpesutarkoituksiin sekä terrorismin rahoitukseen 26. lokakuuta 2005 annettu Euroopan parlamentin ja neuvoston direktiivi 2005/60/EY ⁽⁴⁰⁾ on tästä esimerkkinä. Toinen hyvin tunnettu ja paljon keskustelua herättänyt esimerkki koskee SWIFT-tietoja ⁽⁴¹⁾, joita tarvitaan Yhdysvaltain valtionvarainministeriön terrorismin rahoituksen jäljitysohjelmassa.
64. Tietosuojavaltuutettu katsoo, että näihin suuntauksiin olisi Tukholman ohjelmassa kiinnitettävä erityistä huomiota. Niitä voidaan pitää poikkeuksina käyttötarkoituksen rajoittamisen periaatteesta, ja ne ovat usein voimakkaasti yksityisyyteen puuttuvia, sillä näiden tietojen käyttö voi paljastaa paljon henkilöiden toiminnasta. Kaikissa tapauksissa, joissa tällaisia toimenpiteitä ehdotetaan, on oltava vahvaa näyttöä siitä, että tällaisia yksityisyyteen puuttuvia toimenpiteitä tarvitaan. Jos näyttö voidaan antaa, on varmistettava, että yksityisten henkilöiden oikeudet suojataan.
65. Tietosuojavaltuutettu katsoo, että kaupallisiin tarkoituksiin kerättyjen tietojen käyttö lainvalvontatarkoituksiin olisi sallittava vain tiukoin edellytyksin, kuten:

— Tietoja käytetään vain erikseen määriteltyihin ja tapauskohtaisesti vahvistettuihin tarkoituksiin, kuten terrorismin tai vakavan rikollisuuden torjuntaan.

— Tietojen siirto tapahtuu tarjonta- eikä kysyntäjärjestelmää käyttäen ⁽⁴²⁾.

⁽³⁶⁾ Ks. *Prise*-hankkeen yhteydessä kehitetyt suuntaviivat: ”Guidelines and criteria for the development, implementation and use of Privacy Enhancing Security Technologies” (<http://www.prise.oew.ac.at>).

⁽³⁷⁾ Parhailla käytettävissä olevilla tekniikoilla tarkoitetaan tietyn toiminnan ja siinä käytettävien menettelytapojen tehokkainta ja edistyneintä astetta, joka osoittaa tiettyjen tekniikoiden käytännön soveltuvuuden käytettäväksi periaatteessa pohjana tietotekniikka- ja tietoturvasovelluksille ja -järjestelmille, joiden on oltava EU:n sääntelykehysten yksityisyys-, tietosuojaja- ja turvallisuusvaatimusten mukaisia.

⁽³⁸⁾ Ks. tietosuojavaltuutetun huomautukset eurooppalaisten tietokantojen yhteentoimivuutta koskevasta komission tiedonannosta, 10.3.2006, saatavilla seuraavassa osoitteessa: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

⁽³⁹⁾ Ks. myös kohta 15 edellä.

⁽⁴⁰⁾ EUVL L 309, 25.11.2005, s. 15.

⁽⁴¹⁾ Ks. 29 artiklan mukaisen työryhmän lausunto 10/2006 henkilö tietojen käsittelystä SWIFT-verkossa (Society for Worldwide Interbank Financial Telecommunication).

⁽⁴²⁾ Tarjontajärjestelmässä rekisterinpitäjä lähettää tiedot pyynnöstä lainvalvontaviranomaiselle. Kysyntäjärjestelmässä lainvalvontaviranomaisella on pääsy rekisterinpitäjän tietokantaan, ja se poimii tiedot tästä tietokannasta. Kysyntäjärjestelmässä rekisterinpitäjän on vaikeampi ottaa vastuuta.

- Tiedonsaantipyynnöiden on oltava oikeasuhteisia ja tarkkaan kohdistettuja, ja niiden on periaatteessa perustuttava erityisiin henkilöihin kohdistuviin epäilyihin.
- Rutiininomaisia hakuja, tietojen louhintaa ja profilointia olisi vältettävä.
- Kaikki tietojen käyttö lainvalvontatarkoituksiin olisi kirjattava, jotta oikeuksiaan käyttävä rekisteröity sekä tietosuojaviranomaiset ja oikeusviranomaiset voisivat valvoa tehokkaasti tietojen käyttöä.

VI.3 Tietojärjestelmät ja EU:n elimet

Keskitettyä säilytystä käyttävät ja muut tietojärjestelmät ⁽⁴³⁾

66. EU:n lainsäädäntöön perustuvien tietojärjestelmien määrä on viime vuosina lisääntynyt huomattavasti vapauden, turvallisuuden ja oikeuden alueella. Joskus päätetään sellaisen järjestelmän perustamisesta, johon kuuluu tietojen säilyttäminen keskitetysti Euroopan tasolla, toisissa tapauksissa taas lainsäädännössä edellytetään vain tietojenvaihtoa kansallisten tietokantojen välillä. Schengenin tietojärjestelmä on todennäköisesti paras esimerkki järjestelmästä, jossa säilytys on keskitettyä. Neuvoston päätös 2008/615/YOS (Prüm-päätös) ⁽⁴⁴⁾ on tietosuojan kannalta merkittävin esimerkki järjestelmästä, jossa säilytys ei ole keskitettyä, sillä siinä edellytetään laajaa biometristen tietojen vaihtoa jäsenvaltioiden viranomaisten välillä.
67. Tiedonannossa osoitetaan, että tämä suuntaus luoda uusia järjestelmiä jatkuu. Ensimmäinen esimerkki, joka on kohdasta 4.2.2, on tietojärjestelmä, jolla laajennetaan eurooppalaista rikosrekisteritietojärjestelmää (ECRIS) siten, että se kattaa myös muiden kuin EU-maiden kansalaiset. Komissio on jo tilannut tutkimuksen tuomittujen kolmansien maiden kansalaisten luettelosta (European Index for Convicted Third Country Nationals – EICTCN), joka saattaa johtaa keskitettyyn tietokantaan. Toinen esimerkki on sähköisen oikeudenkäytön yhteydessä tapahtuva tietojen vaihto henkilöistä, jotka ovat muiden jäsenvaltioiden maksukyvyttömyysrekistereissä (tiedonannon kohta 3.4.1). Tässä tietojen säilytys ei ole keskitettyä.
68. Hajautetulla järjestelmällä olisi tietosuojan kannalta tiettyjä etuja. Siinä välitetään tietojen kaksinkertainen säilyttäminen sekä jäsenvaltion viranomaisten että keskusjärjestelmän säilyttäessä tietoja, vastuu tiedoista on selvä, kun jäsenvaltion viranomainen toimii rekisterinpitäjänä, ja oikeusviranomaisten ja tietosuojaviranomaisten valvonta voi tapahtua jäsenvaltioiden tasolla. Vaihdettaessa tietoja muiden oikeusjärjestelmien kanssa järjestelmässä on kuitenkin heikkouksia esimerkiksi sen varmistamisessa, että tiedot pidetään ajan tasalla sekä tietojen alkuperämaassa että määrämaassa, ja siinä, miten taataan molemminpuolinen valvonta. Vielä vai-

keampaa on varmistaa vastuu tietojenvaihdossa käytettävästä teknisestä järjestelmästä. Näiltä vaikeuksilta säästyään valitsemalla keskitetty järjestelmä, jossa EU:n elimet vastaavat ainakin järjestelmän joistakin osista (kuten teknisestä infrastruktuurista).

69. Tässä yhteydessä olisi hyödyllistä kehittää sisällölliset perusteet valinnalle keskitetyn ja hajautetun järjestelmän välillä ja varmistaa näin selkeät ja harkitut toimintapoliittiset valinnat konkreettisissa tapauksissa. Näillä perusteilla voidaan vaikuttaa itse järjestelmien toimivuuteen ja kansalaisten tietojen suojaan. Tietosuojavaltuutettu ehdottaa, että Tukholman ohjelmaan sisällytetään suunnitelma kehittää tällaiset perusteet.

Laajamittaiset tietojärjestelmät

70. Tiedonannon kohdassa 4.2.3.2 käsitellään lyhyesti laajamittaisen tietojärjestelmien tulevaisuutta painopisteen ollessa Schengenin tietojärjestelmässä (SIS) ja viisumitietojärjestelmässä (VIS).
71. Kohdassa 4.2.3.2 mainitaan myös jäsenvaltioiden alueelle tuloa ja sieltä poistumista koskeva sähköinen järjestelmä sekä rekisteröityjä matkustajia koskevat ohjelmat. Komissio ilmoitti järjestelmästä aikaisemmin osana varapuheenjohtaja Franco Frattinin aloitteesta esitettyä ”rajapakettia” ⁽⁴⁵⁾. Tietosuojavaltuutettu suhtautui alustavissa huomautuksissaan ⁽⁴⁶⁾ kriittisesti tähän ehdotukseen, koska niin voimakkaasti yksityisyyteen puuttuvan järjestelmän tarvetta olemassa olevien laajojen järjestelmien lisäksi ei ollut osoitettu riittävän hyvin. Tietosuojavaltuutettu ei näe, että tällaisen järjestelmän tarpeesta olisi mitään lisänäyttöä, ja ehdottaa neuvostolle, että tätä ajatusta ei mainittaisi Tukholman ohjelmassa.
72. Tietosuojavaltuutettu haluaa tässä yhteydessä viitata erilaisia EU:n tietojenvaihdon alalla tehtyjä aloitteita koskeviin lausuntoihinsa ⁽⁴⁷⁾, joissa hän on esittänyt useita ehdotuksia ja huomautuksia laajojen tietokantojen käytön vaikutuksista tietosuojaan EU:n tasolla. Hän on muiden kysymysten ohella kiinnittänyt erityistä huomiota siihen, että tarvitaan vahvoja tapauskohtaisia turvajärjestelyjä, sekä suhteellisuuteen ja vaikutusten arviointiin ennen kuin alalla ehdotetaan tai toteutetaan mitään toimenpiteitä. Tietosuojavaltuutettu

⁽⁴³⁾ Keskitetyllä säilytyksellä tarkoitetaan tässä yhteydessä säilyttämistä keskitetysti Euroopan tasolla ja hajautetulla säilytyksellä säilyttämistä jäsenvaltioiden tasolla.

⁽⁴⁴⁾ Ks. alaviite 33.

⁽⁴⁵⁾ Komission tiedonanto ”Euroopan unionin rajaturvallisuuteen liittyvien tulevien toimien valmistelu”, 13.2.2008, KOM(2008) 69 lopullinen.

⁽⁴⁶⁾ Euroopan tietosuojavaltuutetun alustavat huomautukset kolmesta rajavalvontaa koskevasta komission tiedonannosta (KOM(2008) 69, KOM(2008)68 ja KOM(2008)67), 3. maaliskuuta 2008: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

⁽⁴⁷⁾ Erityisesti seuraavat: 23 päivänä maaliskuuta 2005 annettu lausunto 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, ja 19. lokakuuta 2005 annettu lausunto kolmesta ehdotuksesta, jotka koskevat toisen sukupolven Schengenin tietojärjestelmää (SIS-II), EUVL C 91, 19.4.2006, s. 38.

on aina korostanut oikeaa ja tietosuojan mukaista tasapainoa turvallisuusvaatimusten ja järjestelmien kohteena olevien henkilöiden yksityisyyden suojan välillä. Hän on edustanut samaa kantaa toimiessaan järjestelmien keskusosien valvojana.

73. Lisäksi tietosuojavaltuutettu käyttää tätä tilaisuutta korostaakseen, että tarvitaan johdonmukaista lähestymistapaa EU:n tietojenvaihtoon kokonaisuudessaan, mitä tulee oikeudelliseen, tekniseen ja valvonnan johdonmukaisuuteen jo käytössä olevien ja kehitteillä olevien järjestelmien välillä. Nykyisin tarvitaan todellakin selvästi entistä enemmän rohkeaa kokonaisvaltaista näkemystä siitä, miltä EU:n tietojenvaihdon ja laajojen tietojärjestelmien tulevaisuuden tulisi näyttää. Vain tällaisen näkemyksen perusteella voitaisiin mahdollisesti harkita uudelleen jäsenvaltioiden alueelle tuloa ja sieltä poistumista koskevaa sähköistä järjestelmää.
74. Tietosuojavaltuutettu ehdottaa, että Tukholman ohjelmassa mainitaan aikomus kehittää tällainen näkemys, mihin olisi kuuluttava pohdintaa mahdollisesta Lissabonin sopimuksen voimaantulosta ja sen vaikutuksista ensimmäisen ja kolmannen pilarin oikeusperustaan pohjautuviin järjestelmiin.
75. Lopuksi tiedonannossa mainitaan, että perustetaan uusi virasto, jonka pitäisi tiedonannon mukaan saada myös sähköisiä alueelle tulo- ja alueelta poistumisjärjestelmiä koskeva toimivalta. Komissio on tällä välin hyväksynyt ehdotuksen viraston perustamisesta ⁽⁴⁸⁾. Tietosuojavaltuutettu kannattaa tätä ehdotusta periaatteessa, sillä se voi tehostaa näiden järjestelmien toimintaa, myös tietosuojaa. Hän esittää aikanaan lausunnon tästä ehdotuksesta.

Europol ja Eurojust

76. Europolin rooli on mainittu useassa kohdassa tiedonannossa, jossa korostetaan ensisijaisena asiana, että Europolilla on oltava keskeinen tehtävä koordinoinnissa, tietojenvaihdossa ja asiantuntijoiden koulutuksessa. Lisäksi tiedonannon kohdassa 4.2.2 mainitaan viimeaikaiset muutokset Eurojustin ja Europolin välisen yhteistyön oikeuskehityksessä ja ilmoitetaan, että työ Eurojustin vahvistamiseksi jatkuu erityisesti rajatylittävän järjestäytyneen rikollisuuden tutkinnan osalta. Tietosuojavaltuutettu antaa täyden tukensa näille tavoitteille edellyttäen, että tietosuojan turvaavat suojatoimet toteutetaan asianmukaisella tavalla.

⁽⁴⁸⁾ Kesäkuun 24 päivänä 2009 annettu komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi Schengenin tietojärjestelmän (SIS II), viisumitietojärjestelmän (VIS), Eurodacin ja muiden laaja-alaisen vapauden, turvallisuuden ja oikeuden alueeseen liittyvien tietojärjestelmien operatiivisesta hallinnoinnista vastaavan viraston perustamisesta (KOM(2009) 293/2).

77. Tietosuojavaltuutettu panee tässä yhteydessä tyytyväisenä merkille, että Europolin ja Eurojustin välillä on äskettäin saatu aikaan uusi sopimusluonnos ⁽⁴⁹⁾, jolla pyritään parantamaan ja lisäämään mainittujen elinten keskinäistä yhteistyötä ja turvaamaan niiden välinen tehokas tietojenvaihto. Tehokkaalla tietosuojalla on tässä työssä keskeinen asema.

VI.4 Biometrinen tietojen käyttö

78. Tietosuojavaltuutettu toteaa, että tiedonannossa ei käsitellä kysymystä biometrinen tietojen lisääntyvästä käytöstä Euroopan unionin eri oikeudellisissa välineissä, jotka koskevat tietojenvaihdon toteuttamista, mukaan lukien välineet, joilla perustetaan laaja-alaisia tietojärjestelmiä. Se on valitettavaa ottaen huomioon, että kysymys on tietosuojan ja yksityisyyden suojan kannalta erityisen tärkeä ja arkaluonteinen.
79. Vaikka tietosuojavaltuutettu tunnustaa biometriikan käytön yleisen hyödyllisyyden, hän on jatkuvasti korostanut tällaisten tietojen käytöstä johtuvia huomattavia seurauksia henkilöiden oikeuksien kannalta ja ehdottanut, että kuhunkin järjestelmään sisällytetään tiukat biometriikan käyttöä koskevat suojatoimet. Euroopan ihmisoikeustuomioistuimen äskettäinen tuomio asiassa *S. ja Marper v. Yhdistynyt kuningaskunta* ⁽⁵⁰⁾ antaa tässä yhteydessä hyödyllisiä viitteitä erityisesti biometrinen tietojen käytön perusteluista ja rajoituksista. Erityisesti DNA-tietojen käyttö voi paljastaa henkilöistä arkaluonteisia tietoja, kun otetaan vielä huomioon, että tekniset mahdollisuudet hyödyntää DNA-tietoja lisääntyvät edelleen. Jos tietojärjestelmissä käytetään laajamittaisesti biometrisiä tietoja, ongelmana ovat myös sisäänrakennetut epätasällisyydet biometrinen tietojen keräämisessä ja vertailussa. EU:n lainsäätäjän olisi näistä syistä suhtauduttava pidättyvästi kyseisten tietojen käyttöön.
80. Viime vuosina on myös useasti tullut esille kysymys lasten ja iäkkäiden henkilöiden sormenjalkien käytöstä, koska näitä ikäryhmiä koskevissa biometrisissä järjestelmissä on sisäänrakennettuja heikkouksia. Tietosuojavaltuutettu on pyytänyt perusteellista tutkimusta järjestelmien luotettavuuden tutkimiseksi asianmukaisesti ⁽⁵¹⁾. Hän on ehdottanut lasten osalta ikäraja 14 vuotta, ellei tutkimus anna aihetta muuttaa sitä. Tietosuojavaltuutettu suosittelee, että asia mainitaan Tukholman ohjelmassa.

⁽⁴⁹⁾ Sopimusluonnos, jonka neuvosto on hyväksynyt ja joka molempien osapuolten on vielä allekirjoitettava. Ks. neuvoston rekisteri:

<http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf>
<http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf>

⁽⁵⁰⁾ Yhteiskanne 30562/04 ja 30566/04, *S. ja Marper v. Yhdistynyt kuningaskunta*, 4. joulukuuta 2008 annettu tuomio, Euroopan ihmisoikeustuomioistuin, ei vielä julkaistu.

⁽⁵¹⁾ Maaliskuun 26 päivänä 2008 annettu lausunto ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista annetun neuvoston asetuksen (EY) N:o 2252/2004 muuttamisesta, EUVL C 200, 6.8.2008, s. 1.

81. Tietosuojavaltuutettu katsoo kaikesta huolimatta, että biometristen tietojen käytölle olisi hyödyllistä kehittää sisällölliset perusteet. Niillä olisi varmistettava, että tietoja käytetään ainoastaan silloin, kun se on tarpeellista, asianmukaista ja oikeasuhteista, ja kun lainsäätävä on osoittanut selvän, täsmällisen ja oikeutetun tarkoituksen. Tarkemmin sanottuna, biometrisiä tietoja ja erityisesti DNA-tietoja ei pitäisi käyttää, jos samaan tulokseen voidaan päästä käyttämällä muita, vähemmän arkaluonteisia tietoja.

VII OIKEUSSUOJAN SAATAVUUS JA SÄHKÖINEN OIKEUS

82. Teknologiaa käytetään myös välineenä oikeudellisen yhteistyön parantamiseen. Tiedonannon kohdassa 3.4.1 sähköisen oikeuden todetaan parantavan kansalaisten oikeussuojan saatavuutta. Se muodostuu tietoportaalista ja videokonferensseista osana oikeudellista menettelyä. Se mahdollistaa myös verkko-oikeuskäsittelyn sekä kansallisten rekisterien, kuten maksukyvyttömyysrekisterien yhteenliittämisen. Tietosuojavaltuutettu panee merkille, että tiedonannossa ei mainita uusia sähköistä oikeutta koskevia aloitteita, vaan vahvistetaan jo aloitettuja toimia. Tietosuojavaltuutettu osallistuu joihinkin näistä toimista osana 19. joulukuuta 2008 antamansa komission tiedonantoa ”Tavoitteena sähköisen oikeudenkäytön strategia Euroopalle” koskevan lausunnon⁽⁵²⁾ seuranta.

83. Sähköinen oikeus on kunnianhimoinen hanke, joka tarvitsee täyden tuen. Sillä voidaan parantaa tehokkaasti Euroopan oikeusjärjestelmää ja kansalaisten oikeussuojaa. Se on merkittävä askel kohti Euroopan oikeusaluea. Myönteisestä suhtautumisesta huolimatta voidaan esittää joitakin huomautuksia:

- Sähköisen oikeuden tekniset järjestelmät olisi suunniteltava ”sisäänrakennetun yksityisyyden suojan” periaatetta noudattaen. Kuten edellä eurooppalaisen tiedonhallintamallin yhteydessä todettiin, oikean arkkitehtuurin valitseminen on kaiken lähtökohta.
- Järjestelmien liittämisessä ja yhteentoimivuudessa olisi noudatettava käyttötarkoituksen rajoittamisen periaatetta.
- Eri toimijoiden tehtävät olisi määriteltävä täsmällisesti.
- Arkaluonteisia tietoja sisältävien kansallisten rekisterien, kuten maksukyvyttömyysrekisterien yhteenliittämisestä kansalaisille aiheutuvat seuraukset olisi analysoitava edeltä käsin.

VIII PÄÄTELMÄT

84. Tietosuojavaltuutettu hyväksyy sen, että tiedonannossa painotetaan perusoikeuksien suojaa, erityisesti henkilötietojen suojaa yhtenä keskeisistä kysymyksistä vapauden, turvallisuuden ja oikeuden alueen tulevaisuuden kannalta. Tieto-

sojavaltautettu katsoo, että tiedonannossa aivan oikein edistetään tasapainoa siinä, että toisaalta tarvitaan asianmukaisia välineitä kansalaisten turvallisuuden takaamiseksi ja että toisaalta kansalaisten perusoikeuksien suoja olisi taattava. Siinä tunnustetaan, että henkilötietojen suoja olisi korostettava enemmän.

85. Tietosuojavaltuutettu kannattaa tiedonannon kohtaa 2.3, jossa toivotaan kattavaa tietosuojajärjestelmää, joka käsittäisi kaikki EU:n toimivaltaan kuuluvat alat Lissabonin sopimuksen voimaantulosta riippumatta. Hän suosittelee tässä yhteydessä, että

- Tukholman ohjelmassa ilmaistaan, että tarvitaan selkeää pitkän aikavälin visiota tällaisesta kattavasta järjestelmästä;
- arvioidaan alalla hyväksytyjä toimenpiteitä, niiden toteutusta käytännössä ja niiden tehokkuutta ottaen huomioon niistä yksityisyydelle aiheutuvat haitat ja niiden tehokkuus lainvalvonnan kannalta;
- otetaan yhdeksi Tukholman ohjelman painopisteeksi, että tarvitaan uusi lainsäädäntökehys, jolla muun muassa korvataan neuvoston puitepäättös 2008/977/YOS.

86. Tietosuojavaltuutettu on tyytyväinen komission aikomukseen vahvistaa tietosuojaperiaatteet. Tämän on liityttävä julkiseen kuulemiseen, josta komissio ilmoitti aiheesta ”Personal data — more use, more protection?” 19. ja 20. toukokuuta 2009 järjestetyssä konferenssissa. Sisällön osalta tietosuojavaltuutettu korostaa käyttötarkoituksen rajoittamisen periaatteen merkitystä tietosuojalainsäädännön kulmakivenä ja keskittymistä mahdollisuuksiin parantaa tietosuojaperiaatteiden soveltamisen tehokkuutta välineillä, joilla voidaan lisätä rekisterinpitäjien velvollisuuksia.

87. Sisäänrakennettua yksityisyyden suojaa ja yksityisyyden huomioon ottavia teknologioita voidaan edistää

- tietojärjestelmien rakentajille ja käyttäjille valinnaisena tarjottavalla yksityisyyden ja tietosuojan sertifiointijärjestelmällä
- tietojärjestelmien rakentajille ja käyttäjille asetetulla velvoitteella käyttää järjestelmiä, jotka ovat sisäänrakennetun yksityisyyden suojan periaatteen mukaisia.

88. Tietosuojan ulkoisten näkökohtien osalta tietosuojavaltuutettu suosittelee, että

- Tukholman ohjelmassa korostetaan Yhdysvaltojen ja muiden kolmansien maiden kanssa tietosuojasta ja tietojenvaihdosta tehtävien yleisten sopimusten merkitystä;

⁽⁵²⁾ Tietosuojavaltuutetun 19. joulukuuta 2008 antama lausunto komission tiedonannosta ”Tavoitteena sähköisen oikeudenkäytön strategia Euroopalle”, EUVL C 128, 6.6.2009, s. 13.

- tuetaan aktiivisesti perusoikeuksien ja erityisesti tietosuojan kunnioittamista suhteissa kolmansien maihin ja kansainvälisiin järjestöihin;
 - mainitaan Tukholman ohjelmassa, että henkilötietojen vaihto kolmansien maiden kanssa edellyttää suojan riittävää tasoa tai muita asianmukaisia suojatoimia kyseisissä kolmansissa maissa.
89. Tietosuojavaltuutettu panee suurella mielenkiinnolla merkille kehityksen kohti Euroopan unionin tiedonhallintastrategiaa ja eurooppalaista tiedonhallintamallia ja korostaa, että näissä hankkeissa olisi kiinnitettävä huomiota tietosuojanäkökohtiin, joita olisi kehitettävä edelleen Tukholman ohjelmassa. Tietojenvaihdon arkkitehtuurin olisi perustuttava sisäänrakennettuun yksityisyyden suojaan ja parhaisiin käytävissä oleviin tekniikoihin.
90. Pelkästään se, että on teknisesti mahdollista vaihtaa digitaalisia tietoja yhteentoimivien tietokantojen välillä tai yhdistää tietokantoja, ei anna oikeutta poiketa käyttötarkoituksen rajoittamisen periaatteesta. Yhteentoimivuuden olisi konkreettisesti tapauksissa perustuttava selkeisiin ja harkittuihin toimintapoliittisiin valintoihin. Tietosuojavaltuutettu ehdottaa, että tämä täsmennetään Tukholman ohjelmassa.
91. Tietosuojavaltuutettu katsoo, että kaupallisiin tarkoituksiin kerättyjen tietojen käyttö lainvalvontatarkoituksiin olisi sallittava vain tiukoin edellytyksin, jotka on määritelty tämän lausunnon 65 kohdassa.
92. Lisäksi esitetään muun muassa seuraavia, henkilöitä koskevien tietojen käyttöön liittyviä ehdotuksia:
- Kehitetään sisällölliset perusteet valinnalle keskitetyn ja hajautetun järjestelmän välillä ja sisällytetään Tukholman ohjelmaan suunnitelma kehittää tällaiset perusteet.
 - Sähköisen järjestelmän kehittämistä jäsenvaltioiden alueelle tuloa ja sieltä poistumista varten sekä rekisteröityjä matkustajia koskevia ohjelmia ei pitäisi mainita Tukholman ohjelmassa.
 - Tuetaan Europolin ja Eurojustin vahvistamista ja äskettäin laadittua Europolin ja Eurojustin välistä uutta sopimusta.
 - Kehitetään sisällölliset perusteet biometristen tietojen käytölle sen varmistamiseksi, että tietoja käytetään ainoastaan silloin, kun se on tarpeellista, asianmukaista ja oikeasuhteista ja kun lainsäätäjä on osoittanut selvän, täsmällisen ja oikeutetun tarkoituksen. DNA-tietoja ei pitäisi käyttää, jos samaan tulokseen voidaan päästä käyttämällä muita, vähemmän arkaluonteisia tietoja.
93. Tietosuojavaltuutettu kannattaa sähköistä oikeutta ja on esittänyt joitakin huomautuksia siitä, miten hanketta voitaisiin parantaa (ks. kohta 83).

Tehty Brysselissä 10 päivänä heinäkuuta 2009.

Peter HUSTINX
Euroopan tietosuojavaltuutettu