EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS

Europos duomenų apsaugos priežiūros pareigūno nuomonė

— dėl pasiūlymo dėl Tarybos sprendimo dėl antros kartos Šengeno informacinės sistemos (SIS II) sukūrimo, veikimo ir naudojimo (KOM (2005) 230 galutinis);

— pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl antros kartos Šengeno informacinės sistemos (SIS II) sukūrimo, veikimo ir naudojimo (KOM (2005) 236 galutinis) ir

— pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl valstybių narių tarnybų, atsakingų už transporto priemonių registracijos liudijimų išdavimą, prieigos prie antros kartos Šengeno informacinės sistemos (SIS II) (KOM (2005) 237 galutinis)

(2006/C 91/11)

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS,

atsižvelgdamas į Europos bendrijos steigimo sutartį, ypač į jos 286 straipsnį,

atsižvelgdamas į Europos Sąjungos pagrindinių teisių chartiją, ypač į jos 8 straipsnį,

atsižvelgdamas į 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo,

atsižvelgdamas į 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, ypač į jo 41 straipsnį,

atsižvelgdamas į 2005 m. birželio 17 d. gautą Komisijos prašymą pateikti nuomonę laikantis Reglamento (EB) Nr. 45/2001 28 straipsnio 2 dalies,

PRIĖMĖ ŠIĄ NUOMONĘ:

1. ĮVADAS

1.1. Bendra informacija

Šengeno informacinė sistema (SIS) — tai visą ES apimanti IT sistema, sukurta kaip kompensacinė priemonė Šengeno erdvėje panaikinus vidinių sienų kontrolę. SIS suteikia galimybę valstybių narių kompetentingoms institucijoms keistis informacija, kuri naudojama prie išorinių sienų ar valstybių teritorijoje tikrinant asmenis ir daiktus bei išduodant vizas ir leidimus gyventi.

Šengeno konvencija kaip tarpvyriausybinis susitarimas įsigaliojo 1995 m. Amsterdamo sutartimi Šengeno konvencijos dalis — SIS — buvo vėliau integruota į ES sistemą.

Nauja „antros kartos“ Šengeno informacinė sistema II pakeis dabartinę sistemą, tokiu būdu sudarydama sąlygas išplėsti Šengeno erdvę, į ją įtraukiant naujas ES valstybes nares. Ji taip pat papildys sistemą naujomis funkcijomis. Tarpvyriausybiniu lygiu parengtos Šengeno konvencijos nuostatos bus visapusiškai pakeistos įprastais Europos teisės aktais.

2005 m. birželio 1 d. Europos Komisija pateikė tris pasiūlymus dėl SIS II sukūrimo. Tai:

— pasiūlymas dėl reglamento, grindžiamo EB sutarties IV antraštine dalimi (vizos, prieglobstis, imigracija ir kitos su laisvu asmenų judėjimu susijusios politikos sritys), kuriuo bus reglamentuojami su SIS II susiję pirmojo ramsčio (imigracija) aspektai, toliau — siūlomas reglamentas;

— pasiūlymas dėl sprendimo, grindžiamo ES sutarties VI antraštine dalimi (policijos ir teisminis bendradarbiavimas baudžiamosiose bylose), kuriuo bus reglamentuojamas SIS naudojimas trečiojo ramsčio tikslais, toliau — siūlomas sprendimas;

— pasiūlymas dėl reglamento, grindžiamo V antraštine dalimi (transportas), konkrečiai susijusio su už transporto priemonių registraciją atsakingų institucijų prieiga prie SIS duomenų; šis pasiūlymas bus nagrinėjamas atskirai (žr. toliau išdėstytą 4.6 punktą).

Verta paminėti, kad per ateinančius mėnesius Komisija išleis komunikatą dėl ES informacijos sistemų (SIS, VIS, Eurodac) tarpusavio sąveikos ir didesnės sinergijos.

SIS II sudaro centrinė duomenų bazė — centrinė Šengeno informacinė sistema (CS-SIS), kurios operatyvinį valdymą užtikrins Komisija, ją sujungiant su kiekvienos valstybės narės nurodytomis nacionalinėmis prieigos vietomis (NI-SIS). SIRENE biurai užtikrina keitimąsi papildoma informacija (su SIS II perspėjimais susijusia informacija, kuri nėra saugoma SIS).

Valstybės narės teiks SIS II duomenis apie asmenis, ieškomus suimti, perduoti arba išduoti, asmenis, ieškomus teismo proceso tvarka, asmenis, kuriuos reikia sekti ar specialiai tikrinti, asmenis, kuriems prie išorinių sienų turi būti uždrausta įvažiuoti, ir pamestus ar pavogtus daiktus. Į SIS įvesti duomenys, vadinami perspėjimais, sudaro sąlygas kompetentingai institucijai nustatyti asmenis ar daiktus.

Išplėtotos naujos SIS II ypatybės: išplėsta prieiga prie SIS (Europolas, *Eurojust*, valstybių prokurorai, transporto priemonių registracijos institucijos), perspėjimų tarpusavio susiejimas, papildymas naujomis duomenų kategorijomis, įskaitant biometrinius duomenis (pirštų atspaudus ir nuotraukas) bei techninė platforma, kuria bus dalijamasi su Vizų informacine sistema. Dėl tokių papildymų kilo keletą metų besitęsiančios diskusijos apie SIS paskirties keitimą — iš kontrolės priemonės į pranešimų ir tyrimų sistemą.

1.2. **Bendras pasiūlymų įvertinimas**

1. EDAPP palankiai vertina tai, kad su juo konsultuojamasi pagal Reglamento (EB) Nr. 45/2001 28 straipsnio 2 dalį. Tačiau atsižvelgiant į 28 straipsnio 2 dalies privalomąjį pobūdį, ši nuomonė turėtų būti paminėta tekstų preambulėje.

2. EDAPP palankiai vertina pasiūlymus dėl kelių priežasčių. Tarpvyriausybiniu lygiu nustatytą struktūrą pakeitus Europos teisės aktais, atsiranda keletas teigiamų pasekmių: taps aiškesnė SIS II reglamentuojančių taisyklių teisinė vertė, Teisingumo Teismas bus kompetentingas aiškinti pirmojo ramsčio teisės aktus, Europos Parlamentas bent iš dalies galės dalyvauti (procese, nors ir šiek tiek vėliau).

3. Be to, iš esmės pasiūlymuose daug dėmesio skiriama duomenų apsaugai, o kai kuriose nuostatose pateikiami pageidautini patobulinimai lyginant su esama padėtimi. Visų pirma paminėtinos priemonės, palankios nukentėjusiems nuo tapatybės vagysčių, VI antraštinėje dalyje numatytas Reglamento 45/2001 taikymo išplėtimas Komisijos duomenų tvarkymo veiklai, geresnis perspėjimų dėl draudimo asmenims įvažiuoti motyvų apibrėžimas.

4. Taip pat akivaizdu, kad pasiūlymai buvo rengiami labai kruopščiai; jie yra sudėtingi, bet tai atspindi būdingą jų reglamentuojamos sistemos sudėtingumą. Daugeliu šioje nuomonėje išdėstytų pastabų siekiama patikslinti ar papildyti nuostatas, tačiau nereikalaujama jų visiškai parengti iš naujo.

Vis dėlto, nepaisant šio iš esmės teigiamo įvertinimo, galima pareikšti keletą išlygų visų pirma dėl šių klausimų:

1. Daugeliu atvejų sunku suprasti, kokiu ketinimu remiantis buvo rengiamas tekstas; tenka labai apgailestauti, kad nėra paaiškinamojo memorandumo. Atsižvelgiant į šių dokumentų sudėtingumą, tai būtų pagrindinis reikalavimas. Nesant tokio memorandumo, kai kuriais atvejais skaitytojui belieka tik spėlioti.

2. Be to, tenka apgailestauti, kad neatliktas poveikio įvertinimo tyrimas. Tai, kad pirmoji sistemos versija jau parengta, nepateisina tyrimo nebuvimo, kadangi abi sistemos smarkiai skiriasi. Be kita ko, reikėjo geriau apsvarstyti biometrinių duomenų įvedimo poveikį.

3. Teisinių duomenų apsaugos sistema yra labai sudėtinga; ji remiasi bendru *les generalis* ir *lex specialis* taikymu. Reikėtų užtikrinti, kad net parengus konkrečius teisės aktus, Direktyvoje 95/46/EB ir Reglamente 45/2001 numatytos su duomenų apsauga susijusios nuostatos ir toliau būtų visapusiškai taikomos. Dėl įvairių teisės aktų bendro taikymo neturėtų kilti nacionaliniu lygiu nustatytos tvarkos, susijusios su pagrindiniais aspektais, skirtumų ir sumažėti esamas duomenų apsaugos lygis.

4. Naujoms institucijoms, kurios neatitinka pradinio asmenų ir daiktų tikrinimo tikslo, suteikiamai prieigai turėtų būti taikomos griežtesnės apsaugos priemonės.

5. Pasiūlymai daugiausia grindžiami kitais teisiniais dokumentais, kurie vis dar rengiami (o kartais dar net nepasiūlyti). EDAPP supranta teisėkūros sunkumus sudėtingoje ir nuolat kintančioje aplinkoje; tačiau, atsižvelgiant į atitinkamų asmenų patiriamas pasekmes ir tokios padėties sukuriamą teisinį netikrumą, tokią padėtį jis laiko nepriimtina.

6. Atsiranda tam tikras neapibrėžtumas priskiriant kompetenciją valstybėms narėms ir Komisijai. Aiškumo svarba yra nepaprastai didelė, kadangi jis ne tik būtinas, kad sistema sklandžiai veiktų, bet tai pagrindinis reikalavimas užtikrinant visapusišką sistemos priežiūrą.

1.3. **Nuomonės struktūra**

Nuomonės struktūra tokia: pirmiausia joje paaiškinama SIS II taikytina teisinė bazė. Tuomet apibrėžiamas SIS II tikslas ir pagrindiniai SIS II bei šiuo metu veikiančios sistemos skirtumai. 5 dalyje pateikiamos pastabos apie atitinkamą Komisijos ir valstybių narių vaidmenį, susijusį su SIS II veikimu. 6 dalyje išdėstomos duomenų subjekto teisės, o 7 dalyje aptariama priežiūra nacionaliniu ir EDAPP lygiu bei priežiūros pareigūnų bendradarbiavimas. 8 dalyje pateikiama pastabų ir galimų pakeitimų saugumo srityje; 9 ir 10 dalys atitinkamai susijusios su komitologija ir sąveika. Galiausiai išvadų santraukoje akcentuojamos kiekvienos dalies pagrindinės išvados.

2. ATITINKAMA TEISINĖ BAZĖ

2.1. **Atitinkama SIS II taikoma duomenų apsaugos teisinė bazė**

Direktyva 95/46/EB, Konvencija Nr. 108 ir Reglamentas 45/2001 pasiūlymuose nurodomi kaip duomenų apsaugos teisinė bazė. Taip pat svarbūs ir kiti dokumentai.

Siekiant didesnio aiškumo šioje srityje ir norint priminti pagrindinius nagrinėjimo atramos taškus, tikslinga paminėti šiuos dalykus:

— Pagarba privačiam gyvenimui Europoje buvo užtikrinta 1950 m. Europos Tarybai priėmus Žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją (toliau — ŽTPLK). ŽTPLK 8 straipsnyje numatoma kiekvieno asmens „teisė į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas“.

  Pagal 8 straipsnio 2 dalį valdžios institucijos neturi teisės kištis į naudojimąsi šia teise, išskyrus „įstatymo numatytus atvejus“ ir „kai tai būtina demokratinėje visuomenėje“ svarbiems interesams apsaugoti. Europos žmogaus teisių teismo precedentinėje teisėje šios sąlygos suformavo papildomus reikalavimus: šio kišimosi teisinio pagrindo kokybė, bet kokios priemonės proporcingumas ir tinkamų apsaugos nuo piktnaudžiavimo priemonių poreikis.

— Teisė į privatų gyvenimą ir teisė į asmens duomenų apsaugą buvo ne taip seniai nustatytos Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniuose. Pagal Chartijos 52 straipsnį pripažįstama, kad šios teisės gali būti apribotos, jei patenkinamos sąlygos, panašios į pagal ŽTPLK 8 straipsnį taikomas sąlygas.

— ES sutarties 6 straipsnio 2 dalyje numatoma, kad Sąjunga gerbia pagrindines teises, kurias užtikrina ŽTPLK.

Pasiūlymams dėl SIS II tiesiogiai taikytini šie trys teisės aktai:

— 1981 m. sausio 28 d. Europos Tarybos Konvencija Nr. 108 dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (toliau — Konvencija Nr. 108), kurioje nustatyti pagrindiniai asmenų apsaugos tvarkant asmens duomenis principai. Konvenciją Nr. 108 ratifikavo visos valstybės narės. Ji taikoma ir policijos bei teismų srityse vykdomai veiklai. Šiuo metu SIS konvencijai taikoma duomenų apsaugos tvarka nustatyta Konvencijoje Nr. 108 ir 1987 m. rugsėjo 17 d. Europos Tarybos Ministrų Komiteto rekomendacijoje Nr. R (87) 15, reglamentuojančioje asmens duomenų naudojimą policijos veiklos srityje.

— 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, p. 31). Ši direktyva toliau vadinama Direktyva 95/46/EB. Verta paminėti, kad daugumoje valstybių narių šią direktyvą įgyvendinantys nacionalinės teisės aktai taip pat apima duomenų tvarkymą, atliekamą policijos ir teisingumo srityse.

— 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, p. 1). Šis reglamentas toliau vadinamas Reglamentu 45/2001.

Direktyvos 95/46/EB ir Reglamento 45/2001 aiškinimas turi iš dalies priklausyti nuo atitinkamos Europos žmogaus teisių teismo precedentinės teisės, laikantis 1950 m. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos. Kitaip tariant, direktyvos ir reglamento nuostatos, susijusios su asmens duomenų tvarkymu, kuris gali pažeisti pagrindines laisves, visų pirma teisę į privatumą, turi būti aiškinamos atsižvelgiant į pagrindines teises. Tą taip pat rodo ir Europos Teisingumo Teismo teisminė praktika ([1]).

([1]) Šiuo atveju naudinga nurodyti Teisingumo Teismo sprendimą *Österreichischer Rundfunk and Others* byloje (jungtinės bylos C-465/00, C-138/01 ir C-139/01, 2003 m. gegužės 20 d. sprendimas, visos sudėties Teismas, (2003), Rink. I-4989). Teismas nagrinėjo Austrijos įstatymą, pagal kurį numatoma perduoti su valstybinio sektoriaus darbuotojų darbo užmokesčiu susijusią informaciją Austrijos audito rūmams ir vėliau ją paskelbti. Savo sprendime Teismas išdėsto daugelį Europos žmogaus teisių konvencijos 8 straipsniu pagrįstų kriterijų, kuriais reikėtų remtis taikant Direktyvą 95/46/EB, nepažeidžiant šia direktyva leidžiamų tam tikrų teisės į privatumą apribojimų.

2005 m. spalio 4 d. Komisija pateikė pasiūlymą dėl Tarybos pamatinio sprendimo dėl asmens duomenų, tvarkomų pagal policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos ([1]) (toliau — pamatinio sprendimo projektas). Šį pamatinį sprendimą ketinama nurodyti sprendimo dėl SIS II projekto teisiniu pagrindu vietoj Konvencijos Nr. 108, nes jis galėtų turėti įtakos duomenų apsaugos tvarkai šioje srityje (žr. toliau išdėstytą 2.2.5 punktą).

2.2. **SIS II duomenų apsaugos teisinė tvarka**

2.2.1. *Bendros pastabos*

SIS II reglamentuoti reikalingą teisinę bazę sudaro atskiri dokumentai; tačiau, kaip nurodyta konstatuojamosiose dalyse, tai „nepažeidžia principo, pagal kurį SIS II laikoma viena bendra informacine sistema ir turi veikti kaip tokia sistema. Todėl tam tikros šių dokumentų nuostatos turėtų būti vienodos."

Abiejų dokumentų struktūra iš esmės yra vienoda, o I–III skyriai abiejuose tekstuose yra beveik identiški. Tai, kad SIS II turi būti laikoma viena bendra informacine sistema, turinčia dvi skirtingas teisines bazes, taip pat atspindėta gana sudėtingoje duomenų apsaugos tvarkoje.

Duomenų apsaugos tvarka iš dalies apibrėžiama pačiuose pasiūlymuose kaip *lex specialis,* kurią papildo įvairūs kiekvieno sektoriaus (pirmajam ramsčiui priklausanti Komisija, valstybės narės, trečiajam ramsčiui priklausančios valstybės narės) teisiniai pagrindai (*lex generalis*).

Dėl tokios struktūros kyla klausimas, koks turėtų būti konkrečių taisyklių ir bendrosios teisės santykis. Šiuo atveju EDAPP mano, kad taikant konkrečią taisyklę taikoma bendra taisyklė. Todėl *lex specialis* visada turi atitikti *lex generalis;* ji išplečia (sukonkretina ar papildo) *lex generalis*, tačiau nelaikoma jos išimtimi.

Kilus klausimui, kokią taisyklę taikyti konkrečiais atvejais, laikomasi principo, kad pirmenybė teikiama *lex specialis;* tačiau kilus neaiškumams, turėtų būti daroma nuoroda į *lex generalis.*

Pagal šią struktūrą išskiriami trys *lex generalis* ir *lex specialis* deriniai. Galima būtų pateikti tokią santrauką.

2.2.2. *Komisijai taikytina tvarka*

Tais atvejais, kai dalyvauja Komisija, taikomas Reglamentas 45/2001, įskaitant EDAPP vaidmenį, neatsižvelgiant į tai, ar veikla turi būti vykdoma, vadovaujantis pirmuoju ramsčiu (siūlomas reglamentas) ar trečiuoju ramsčiu (siūlomas sprendimas). Siūlomo sprendimo 21 konstatuojamojoje dalyje teigiama: „Reglamentas (EB) Nr. 45/2001 (...) taikomas Komisijos tvarkomiems asmens duomenims, kai jie tvarkomi vykdant veiklą, kuri visa ar jos dalis patenka į Bendrijos teisės taikymo sritį. Asmens duomenų tvarkymas SIS II iš dalies priskiriamas Bendrijos teisės taikymo sričiai."

Tam yra praktinės priežastys: iš tiesų būtų nepaprastai sudėtinga Komisijos atveju nustatyti, ar duomenys tvarkomi vykdant pirmojo ar trečiojo ramsčio teisės aktų taikymo sričiai priskiriamus veiksmus.

Be to, taikyti vieną teisės aktą visai Komisijos su SIS II susijusiai veiklai praktiniu požiūriu yra ne tik racionaliau, bet ir nuosekliau (užtikrinant pagal siūlomo reglamento 21 konstatuojamąją dalį „nuoseklų ir vienodą taisyklių, reglamentuojančių asmenų pagrindinių teisių ir laisvių apsaugą, taikymą tvarkant asmens duomenis"). Todėl EDAPP palankiai vertina tai, kad Komisija pripažįsta, jog Reglamentas 45/2001 taikomas visai jos su SIS II susijusiai duomenų tvarkymo veiklai.

2.2.3. *Valstybėms narėms taikytina tvarka*

Padėtis, susijusi su valstybėmis narėmis, yra sudėtingesnė. Asmens duomenų tvarkymą taikant siūlomą reglamentą reglamentuoja pats siūlomas reglamentas ir Direktyva 95/46/EB. Siūlomo reglamento 14 konstatuojamosios dalies formuluotėje aiškiai išdėstoma, kad direktyvą reikia laikyti *lex generalis,* o SIS II reglamentą — *lex specialis*. Iš to kyla keletas pasekmių, kurios bus toliau aptariamos smulkiau.

Siūlomo sprendimo atveju duomenų apsaugos teisinis pagrindas (*lex generalis*) — Konvencija Nr. 108, kurią taikant tam tikrais atvejais gali labai skirtis pirmojo ir trečiojo ramsčių duomenų apsaugos tvarka.

2.2.4. *Poveikis duomenų apsaugos lygiui*

Pateikdamas bendrą pastabą dėl tokios duomenų apsaugos struktūros, EDAPP pabrėžia šiuos dalykus:

— Tai, kad siūlomas reglamentas naudojamas kaip Direktyvos 95/46/EB *lex specialis* (analogiškai, siūlomas sprendimas naudojamas kaip Konvencijos Nr. 108 *lex specialis*), neturėtų sumažinti pagal direktyvą ar konvenciją užtikrinto duomenų apsaugos lygio. Šiuo tikslu EDAPP pateiks rekomendacijų (žr., pavyzdžiui, teisę į teisės gynimo priemones).

([1]) 2 (KOM(2005) 475 galutinis).

— Analogiškai, bendrai taikant teisės aktus negali sumažėti pagal galiojančią Šengeno konvenciją užtikrintas duomenų apsaugos lygis (žr., pavyzdžiui, toliau išdėstytas pastabas dėl Direktyvos 95/46/EB 13 straipsnio).

— Taikant du skirtingus teisės aktus, kadangi tai būtina dėl Europos teisinės sistemos, neturėtų atsirasti atitinkamų asmenų duomenų apsaugos nepagrįstų skirtumų pagal su jais susijusių tvarkomų duomenų rūšis. To reikia kuo labiau vengti. Toliau pateikiamomis rekomendacijomis taip pat bus siekiama kuo labiau padidinti nuoseklumą (žr., pavyzdžiui, nacionalinių priežiūros institucijų įgaliojimus).

— Teisinė sistema yra tokia sudėtinga, kad labai tikėtina, jog tai sukels tam tikrą sumaištį praktiškai taikant teisės aktus. Kai kuriais atvejais sunku suprasti *lex generalis* ir *lex specialis* sąveiką ir būtų naudinga pasiūlymuose tai paaiškinti. Be to, tokioje sudėtingoje teisinėje aplinkoje labai vertingas Šengeno bendros priežiūros institucijos (BPI) 2005 m. rugsėjo 27 d. „nuomonėje dėl siūlomos SIS II teisinės bazės“ pateiktas pasiūlymas sukurti žinyną, kuriame būtų išvardintos visos su SIS II susijusios teisės ir nurodyta aiški taikomų teisės aktų hierarchija.

Taigi šia nuomone bus siekiama užtikrinti aukšto lygio duomenų apsaugą, nuoseklumą ir aiškumą, kad duomenų subjektui būtų suteiktas reikalingas teisinis tikrumas.

2.2.5. *Pamatinio sprendimo projekto poveikis duomenų apsaugai trečiojo ramsčio srityje*

Konvencija Nr. 108 kaip Sprendimo dėl SIS II projekto teisinė bazė duomenų apsaugos srityje bus keičiama Pamatiniu sprendimu dėl duomenų apsaugos trečiojo ramsčio srityje [1]. Pasiūlyme to nėra paminėta, tačiau tai paaiškėja iš siūlomo pamatinio sprendimo. Pamatinio sprendimo 34 straipsnio 2 dalyje numatoma, kad „bet kokia nuoroda į 1981 m. sausio 28 d. Europos Tarybos Konvenciją Nr. 108 dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu yra laikoma nuoroda į šį pamatinį sprendimą.“ Per ateinančias savaites EDAPP pateiks nuomonę dėl pamatinio sprendimo projekto, o šioje nuomonėje pamatinio sprendimo projekto turinio išsamiai nenagrinės. Tačiau nuomonėje bus paminėti atvejai, kai tikėtina, jog pamatinio sprendimo taikymas turės didelės įtakos SIS II duomenų apsaugos tvarkai.

2.2.6. *Direktyvos 95/46/EB 13 straipsnio ir Konvencijos Nr. 108 9 straipsnio taikymas*

Direktyvos 95/46/EB 13 straipsnyje ir Konvencijos Nr. 108 9 straipsnyje numatoma galimybė valstybėms narėms imtis teisinių priemonių apriboti jiems taikomas pareigas ir teises tais atvejais, kai toks apribojimas yra būtina priemonė kitiems svarbiems interesams apsaugoti (pvz., nacionalinis saugumas, gynyba, visuomenės saugumas) [2].

Siūlomo reglamento ir siūlomo sprendimo konstatuojamosiose dalyse nurodoma, kad valstybės narės gali pasinaudoti šia galimybe įgyvendindamos pasiūlymus nacionaliniu lygiu. Šiuo atveju turėtų būti atliekamas dvigubas patikrinimas: taikant Direktyvos 95/46/EB 13 straipsnį turi būti laikomasi ŽTPLK 8 straipsnio ir neturėtų būti švelninama esama duomenų apsaugos tvarka.

SIS II atveju tai yra net svarbiau, nes sistema turi būti nuspėjama. Kadangi valstybės narės dalijasi duomenimis, turi būti suteikta galimybė pakankamai aiškiai žinoti, kaip jie bus tvarkomi nacionaliniu lygiu.

Šiuo atveju atsiranda ypač nerimą keliantis klausimas, ar dėl pasiūlymų nesumažės esamas duomenų apsaugos lygis. Šengeno konvencijos 102 straipsnyje numatyta sistema, kuri griežtai reglamentuoja ir riboja duomenų naudojimą net pagal nacionalinę teisę („Bet koks duomenų naudojimas, neatitinkantis šio straipsnio 1–4 dalių nuostatų, pagal kiekvienos Susitariančiosios Šalies įstatymus laikomas piktnaudžiavimu“). Tačiau Direktyvoje 95/46/EB ir Konvencijoje Nr. 108 nustatyta, kad nacionalinėje teisėje gali būti numatytos *inter alia* tikslo ribojimo principo išimtys. Taip atsitikus, atsirastų neatitikimų su Šengeno konvencijoje numatyta esama sistema, pagal kurią nacionalinė teisė negali nukrypti nuo tikslo ir naudojimo ribojimo pagrindinio principo.

Priėmus pamatinį sprendimą, ši pastaba liktų nepakitusi: daugiau sunkumų kyla išlaikyti SIS II duomenis tvarkant taikomą griežtą tikslo ribojimo principą nei užtikrinti, kad duomenys būtų tvarkomi laikantis pamatinio sprendimo.

[1] Jis taip pat pakeis Šengeno konvencijos bendrą duomenų apsaugos tvarką (Šengeno konvencijos 126–130 straipsniai). Ši tvarka SIS netaikoma.

[2] Valstybė narė gali pasinaudoti galimybe apriboti teises tik laikydamasi ŽTPLK 8 straipsnio, kaip minėta pirmiau.

EDAPP siūlo SIS II pasiūlymus (visų pirma siūlomo reglamento 21 straipsnį ir siūlomo sprendimo 40 straipsnį) papildyti panašia nuostata, kaip Šengeno konvencijos 102 straipsnio 4 dalies nuostata, ribojančia valstybių narių galimybę nustatyti SIS II dokumentuose nenumatytų duomenų naudojimą. Kita galimybė — siūlomame sprendime ir siūlomame reglamente aiškiai apriboti išimčių, kurios gali būti naudojamos pagal direktyvos 13 straipsnį ar Konvencijos 9 straipsnį, taikymo sritį, nustatant, pavyzdžiui, kad valstybės narės gali apriboti tik prieigos teisę ir teisę į informaciją, o ne duomenų kokybės principus.

3. TIKSLAS

Pagal abiejų dokumentų 1 straipsnį („SIS II sukūrimas ir bendrasis tikslas“) SIS II sukuriama tam, kad „valstybių narių kompetentingoms institucijoms būtų sudaryta galimybė keistis informacija asmenų ir daiktų kontrolės tikslais“ ir ji „padeda išlaikyti aukšto lygio saugumą erdvėje, neturinčioje vidinių sienų kontrolės tarp valstybių narių“.

SIS II tikslas suformuluotas pakankamai bendrąja prasme; pirmiau minėtose nuostatose nepateikiamas tikslus apibrėžimas, ką apima šis tikslas (kam jis skirtas).

Atrodo, kad SIS II tikslas yra daug visapusiškesnis nei Šengeno konvencijos 92 straipsnyje išdėstytas galiojančios SIS tikslas, kuriame konkrečiai daroma nuoroda į leidimą „(...) prieiti prie perspėjimų dėl asmenų ir daiktų vykdant pasienio kontrolę bei atliekant kitus policijos ir muitinės tikrinimus (...) ir (96 straipsnyje nurodytų perspėjimų atveju) išduodant vizas, leidimus gyventi ir administruojant užsieniečiams taikomus teisės aktus (...)“.

Šis visapusiškesnis tikslas taip pat kyla iš to, kad SIS II papildyta naujomis funkcijomis ir prieigomis, kurių neapima pirminis asmenų ir daiktų kontrolės tikslas, bet kurios labiau priklauso tyrimo priemonei. Visų pirma prieiga numatyta institucijoms, kurios SIS II duomenis naudos savais tikslais, o ne įgyvendindamos SIS II tikslus (žr. toliau); bus apibendrintas perspėjimų tarpusavio susiejimas, o tai policijos tyrimo priemonės tipinis bruožas.

Taip pat kyla klausimų dėl biometrinių duomenų paieškos mechanizmo, kuris turi būti sukurtas per ateinančius metus ir kuris sudarytų sąlygas sistemoje atlikti duomenų paieškas, kurios viršija kontrolės sistemos poreikius.

Taigi pasiūlymai yra gerokai visapusiškesni nei esama sistema. Tam reikia papildomų apsaugos priemonių. Todėl analizuodamas EDAPP daugiausia dėmesio skirs ne 1 straipsnyje pateikiamam plačiam sąvokos apibrėžimui, o SIS II funkcijoms ir kitoms sudedamosioms dalims.

4. SVARBŪS SIS II POKYČIAI

Šiame skyriuje daugiausia dėmesio bus skiriama naujiems SIS II įvestiems dalykams, visų pirma biometrinių duomenų įvedimui, naujai prieigos sąvokai, ypač Europolo ir *Eurojust* prieigai, už transporto priemonių registraciją atsakingoms institucijoms, perspėjimų tarpusavio susiejimui ir įvairių institucijų prieigai prie imigracijos duomenų.

4.1. Biometriniai duomenys

Pasiūlymuose dėl SIS II pateikiama galimybė tvarkyti naujos kategorijos duomenis, kuriems reikia skirti ypatingą dėmesį: tai — biometriniai duomenys. Kaip jau pabrėžta EDAPP nuomonėje dėl Vizų informacinės sistemos ([1]), dėl natūraliai opaus biometrinių duomenų pobūdžio jiems reikia taikyti ypatingas apsaugos priemones, kurios nėra nustatytos pasiūlymuose dėl SIS II.

Apskritai biometrinių duomenų naudojimo ES informacinėse sistemose (VIS, EURODAC, vairuotojų pažymėjimų informacinė sistema ir t.t.) tendencija nuolat auga, tačiau atidus susijusių pavojų ir reikalingų apsaugos priemonių įvertinimas nėra atliekamas.

Montrė įvykusioje tarptautinėje duomenų apsaugos įgaliotinių konferencijoje priimtoje rezoliucijoje dėl biometrinių duomenų ([2]) taip pat pabrėžiamas gilesnio šių klausimų svarstymo poreikis. Iki šiol rengiamų standartų pridėtinė vertė buvo grindžiama tik didėjančia sistemų sąveika, o ne biometrinių procesų kokybės gerinimu.

([1]) EDAPP nuomonė dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl Vizų informacinės sistemos (VIS) ir apsikeitimo duomenimis apie trumpalaikes vizas tarp valstybių narių, 2005 m. kovo 23 d., 3.4.2 punktas.

([2]) 27-oji Tarptautinė duomenų apsaugos ir privatumo įgaliotinių konferencija, Montrė, 2005 m. rugsėjo 16 d., Rezoliucija dėl biometrinių duomenų naudojimo pasuose, tapatybės kortelėse ir kelionės dokumentuose.

Būtų naudinga nustatyti su tokių duomenų specifika susijusius bendrus įpareigojimus ar reikalavimus bei bendrą jų įgyvendinimo metodiką. Tokie bendri reikalavimai galėtų visų pirma apimti šiuos dalykus (kurių poreikį parodė pasiūlymai dėl SIS II):

— **Tikslinis poveikio įvertinimas:** Reikia pabrėžti, kad teikiant pasiūlymus nebuvo atliktas biometrinių duomenų naudojimo poveikio įvertinimas ([1]).

— **Dėmesys duomenų įregistravimo procesui:** Biometrinių duomenų šaltinis ir jų rinkimo būdas nėra smulkiai aprašyti. Duomenų įregistravimas yra nepaprastai svarbus bendram biometrinių duomenų nustatymo procesui ir negali būti nustatomas tik priedais ar tolesnių pogrupių diskusijų metu, kadangi jis turės tiesioginę įtaką galutiniam proceso rezultatui, t.y. klaidingo neatitikimo koeficiento ar klaidingo atitikimo koeficiento lygiui.

— **Dėmesys tikslumui:** Pasiūlyme pateikiamas biometrinių duomenų naudojimas atpažinimui (vieno lyginimas su daugeliu) ateityje įgyvendinant biometrinių duomenų paieškos mechanizmą yra dar svarbesnis, kadangi šio proceso rezultatai nėra tokie tikslūs palyginti su biometrinių duomenų naudojimu autentiškumui nustatyti ar kontrolei (vieno lyginimas su vienu). Todėl biometrinių duomenų naudojimas atpažinimui neturėtų būti vienintelis atpažinimo būdas ar vienintelė galimybė gauti papildomą informaciją.

— **Atsarginė procedūra:** Siekiant pagarbos asmenų, kurie galėjo būti neteisingai atpažinti, orumui ir vengiant jiems užkrauti sistemos trūkumų naštą, turi būti įgyvendinamos lengvai prieinamos atsarginės procedūros.

Biometrinių duomenų naudojimas, iš anksto tinkamai jų neįvertinus, taip pat rodo, kad tokių duomenų patikimumas yra pervertinamas. Biometriniai duomenys yra nepastovūs ir laikui bėgant kinta; duomenų bazėse saugomi pavyzdžiai yra tik dinamiško elemento momentiniai duomenys. Jie nėra visiškai pastovūs ir turi būti kontroliuojami. Biometrinių duomenų tikslumas visada turi būti vertinamas atsižvelgiant į kitus elementus, kadangi jis niekada nebus absoliutus.

([1]) Įvertinimas galėtų būti grindžiamas vadinamaisiais septyniais protingo biometrinių duomenų naudojimo ramsčiais, išdėstytais leidinyje „Biometrics at the frontiers: Assessing the impact on Society“ IPTS, DG-JRC, EUR 21585 EN, 1.2 dalis, p. 32.

Galimas SIS II duomenų naudojimas tyrimo tikslais kelia rimtą pavojų duomenų subjektui, jei biometriniais duomenimis pagrįsti įrodymai laikomi labai svarbiais ar pervertinami, kaip buvo minėta ankstesniais atvejais ([2]).

Todėl pasiūlymuose turėtų būti pripažintos atpažinimui naudojamų biometrinių duomenų realios galimybės ir apie tai suteikiama daugiau informacijos.

4.2. **Prieiga prie SIS II duomenų**

4.2.1 *Nauja prieigos koncepcija*

Kiekvieno perspėjimo atveju nustatomos institucijos, turinčios prieigą prie SIS II duomenų. Iš esmės, suteikiant prieigą prie SIS II duomenų, taikomas dvigubas patikrinimas: prieiga turi būti suteikiama institucijoms, kurios visapusiškai atitinka bendrą SIS II tikslą ir konkretų tikslą kiekvieno perspėjimo atveju.

Tai paaiškėja iš perspėjimo sąvokos apibrėžimo, pateikto siūlomame reglamente ir siūlomame sprendime (abiejų dokumentų 3 straipsnio 1 dalies a punktas: *„perspėjimas“ — į SIS II įvestų duomenų rinkinys, padedantis kompetentingoms institucijoms identifikuoti asmenį arba daiktą, kad dėl jų būtų galima imtis konkrečių veiksmų)*. Siūlomo sprendimo 39 straipsnio 3 dalyje toks požiūris pagrindžiamas numatant, kad *„1 dalyje nurodyti duomenys naudojami tik asmens atpažinimui, atsižvelgiant į konkretų veiksmą, kurio reikia imtis pagal šį sprendimą“*. Todėl SIS II vis dar turi „yra-nėra“ principu veikiančios sistemos požymių, kai kiekvienas perspėjimas įvedamas siekiant konkretaus tikslo (perdavimas, draudimas įvažiuoti ir t.t.).

Institucijų, turinčių prieigą prie SIS duomenų, *de facto* naudojimasis šiais duomenimis ribojamas, kadangi jos iš esmės gali pasinaudoti jais tik konkrečiam veiksmui atlikti.

Tačiau naujuose pasiūlymuose numatytos kai kurios prieigos rūšys nesuderinamos su šia logika: iš tiesų, prieiga suteikiama siekiant institucijai suteikti informaciją, o ne jai sudaryti sąlygas atpažinti asmenį ir imtis perspėjime numatytų veiksmų.

([2]) 2004 m. birželio mėn. vienas Portlendo (JAV) teisininkas buvo įkalintas dviems savaitėms, kadangi jo pirštų antspaudai, FTB manymu, atitiko po Madrido teroro akto rastus pirštų antspaudus (ant plastikinio maišelio, kuriame rastas detonatorius). Galiausiai paaiškėjo, kad atitikimo nustatymo procese buvo trūkumų ir dėl to įvyko klaida.

Tiksliau tai susiję su:

— prieglobsčio suteikimo tarnyboms suteikta prieiga prie imigracijos duomenų;

— už pabėgėlio statuso suteikimą atsakingoms tarnyboms suteikiama prieiga prie imigracijos duomenų;

— Europolui suteikiama prieiga prie perspėjimų dėl ekstradicijos, atsargaus sekimo ir pavogtų konfiskavimo dokumentų;

— *Eurojust* suteikiama prieiga prie ekstradicijos ir lokalizavimo duomenų.

Visos minėtos institucijos yra lygiavertės SIS II duomenų požiūriu:

jos negali imtis konkrečių veiksmų, minėtų perspėjimo sąvokos apibrėžime. Prieiga joms suteikiama tik tam, kad jos savo pačių tikslais pasinaudotų informacija.

Šios institucijos skirstomos į tas, kurioms prieiga suteikiama naudotis savo pačių tikslais, bet gana konkrečiai užduočiai atlikti, ir į tas, kurioms nereikia nurodyti prieigos tikslo (visų pirma Europolas ir *Eurojust*). Prieglobsčio suteikimo institucijos, pavyzdžiui, turi prieigą konkrečiam tikslui, net jeigu tai nėra perspėjime nurodytas tikslas. Joms gali būti suteikta prieiga prie imigracijos duomenų „siekiant nustatyti, ar prieglobsčio prašytojas nelegaliai buvo apsistojęs kitoje valstybėje narėje.“ Tačiau Europolas ir *Eurojust* turi prieigą prie tam tikrų kategorijų perspėjimų duomenų, „kurie jiems reikalingi savo užduotims atlikti“.

Apibendrinant, prieiga prie SIS II duomenų suteikiama trimis atvejais:

— prieiga siekiant įgyvendinti perspėjime numatytus veiksmus;

— prieiga kitais nei SIS II tikslais, kurie yra gerai apibrėžti pasiūlymuose;

— prieiga kitais nei SIS II tikslais, kurie nėra tiksliai apibūdinti.

EDAPP nuomone, kuo bendresnis prieigos tikslas, tuo griežtesnės turėtų būti apsaugos priemonės, kurias reikia įgyvendinti. Bendros apsaugos priemonės smulkiai išvardintos toliau, nagrinėjant ypatingą Europolo ir *Eurojust* padėtį.

4.2.2 *Prieigos suteikimo sąlygos*

1. Prieiga gali būti suteikiama tik tuo atveju, kai ji atitinka bendrą SIS II tikslą ir teisinę bazę.

Tai reiškia, kad suteikiant prieigą prie imigracijos duomenų pagal siūlomą reglamentą praktiškai turi būti remiamas politikos, apimančios Šengeno *acquis* dalį, susijusią su asmenų judėjimu, įgyvendinimas.

Suteikiant sprendime numatytą prieigą prie perspėjimų analogiškai siekiama remti operatyvinį policijos ir teisminių institucijų bendradarbiavimą baudžiamosiose bylose.

Todėl EDAPP atkreipia dėmesį į skyrių, susijusį su tarnybų, atsakingų už registracijos liudijimų išdavimą, prieiga prie SIS II (žr. 4.6 punktą).

2. Turi būti įrodyta, kad prieiga prie SIS II duomenų yra reikalinga ir kad neįmanoma arba labai sudėtinga gauti duomenis kitomis mažiau trikdančiomis priemonėmis. Tai turėjo būti išdėstyta paaiškinamajame memorandume, dėl kurio nebuvimo, kaip jau minėta, tenka labai apgailestauti.

3. Turi būti aiškiai apibrėžta, kokiu tikslu duomenys bus naudojami, ir apribotos jų naudojimo galimybės.

Pavyzdžiui, prieglobsčio suteikimo institucijoms suteikiama prieiga prie imigracijos duomenų „siekiant nustatyti, ar prieglobsčio prašytojas nelegaliai buvo apsistojęs kitoje valstybėje narėje.“ Tačiau Europolas ir *Eurojust* turi prieigą prie tam tikrų kategorijų perspėjimų duomenų, „kurie jiems reikalingi savo užduotims atlikti“: tai nėra pakankamai išsamiai paaiškinta (žr. toliau).

4. Prieigos suteikimo sąlygos turi būti gerai apibrėžtos ir apribotos. Visų pirma prieiga prie SIS II duomenų turėtų būti suteikiama tik tų organizacijų padaliniams, dirbantiems su SIS II duomenimis. Šią siūlomo sprendimo 40 straipsnyje ir siūlomo reglamento 21 straipsnio 2 dalyje išdėstytą prievolę reikėtų papildyti nacionalinių institucijų prievole turėti atnaujinamą asmenų, kuriems suteikta prieigos prie SIS II teisė, sąrašą. Tai turėtų būti taikoma ir Europolui bei *Eurojust*.

5. Tai, kad šioms institucijoms suteikta prieiga prie SIS II duomenų, niekada negali būti laikoma pagrindu įvesti duomenis į sistemą arba juos ten laikyti, jeigu jie nėra naudingi konkrečiam perspėjimui, kurio dalimi jie yra. Negalima įvesti naujų duomenų kategorijų dėl to, kad jie būtų naudingi kitoms informacinėms sistemoms. Pavyzdžiui, siūlomo sprendimo 39 straipsnyje numatoma perspėjimus papildyti duomenimis apie juos pateikusias institucijas. Šių duomenų nereikia veiksmams atlikti (areštui, sekimui ir t.t.) ir vienintelė priežastis, kodėl juos galima būtų įvesti, yra tai, kad jie greičiausiai būtų naudingi Europolui ir *Eurojust*. Reikėtų pateikti aiškų tokių duomenų tvarkymo pagrindimą.

6. Duomenų saugojimo laikotarpio pratęsti negalima, išskyrus atvejus, kai tai būtina tuo tikslu, kuriuo duomenys buvo įvesti. Tai reiškia, kad net jei Europolas ar *Eurojust* turi prieigą prie šių duomenų, tai nėra pakankamas pagrindas juos laikyti sistemoje (pavyzdžiui, išdavus ieškomą asmenį, duomenis reikėtų ištrinti, net jeigu jie galėtų būti naudingi Europolui). Šiuo atveju reikės atidžiai prižiūrėti, kad tokį principą taikytų nacionalinės institucijos.

4.2.3. *Europolo ir Eurojust prieiga*

a) *Prieigos suteikimo pagrindas*

Dėl Europolo ir *Eurojust* prieigos prie kai kurių SIS II duomenų jau buvo diskutuota, prieš tai nustatant 2005 m. vasario 24 d. Tarybos sprendimu [1]. Tarp visų institucijų, kurioms suteikta prieiga savo tikslais, minėtos institucijos naudojasi prieiga labiausiai neapibrėžtomis sąlygomis. Nors šių duomenų naudojimas apibrėžtas sprendimo XII skyriuje, prieigos suteikimo pagrindas pirmiausia nėra pakankamai paaiškintas. Tuo labiau, kad tikėtina, jog Europolo ir *Eurojust* užduotys laikui bėgant išsiplės.

EDAPP primygtinai reikalauja, kad Komisija apribotų užduotis, kurioms atlikti būtų pagrįsta Europolo ir *Eurojust* prieiga.

b) *Duomenų apribojimas*

Siekiant išvengti to, kad Europolas ir *Eurojust*„žvejotų“ duomenis, ir užtikrinti tai, kad prieiga būtų suteikiama tik prie tų duomenų, „kurie jiems reikalingi savo užduotims atlikti“, 2005 m. rugsėjo 27 d. nuomonėje dėl pasiūlymų dėl SIS II Šengeno bendra priežiūros institucija pasiūlė apriboti Europolo ir *Eurojust* prieigą prie duomenų apie asmenis, kurių pavardės jau yra įtrauktos į jų dokumentų bylas. Tai užtikrintų naudojimąsi tik jiems aktualiais perspėjimais. EDAPP remia šią rekomendaciją.

c) *Saugumo aspektai*

EDAPP palankiai vertina prievolę registruoti visus veiksmus, kuriuos Europolas ir *Eurojust* atlieka prisijungdami prie sistemos, bei draudimą kopijuoti ar perkelti sistemos dalis.

Siūlomo sprendimo 56 straipsnyje numatoma Europolui ir *Eurojust* suteikti „vieną arba dvi“ prieigos vietas. Kad ir koks aiškus būtų valstybės narės poreikis turėti daugiau nei vieną prieigos vietą dėl to, kad jos kompetentingos institucijos nėra centralizuotos, Europolo ir *Eurojust* statusas ir veikla tokio prašymo nepagrindžia. Be to, reikia pabrėžti, kad saugumo prasme didesnis prieigos vietų skaičius padidina netinkamo naudojimo riziką ir todėl turėtų būti tiksliai pagrįstas nuoseklesniais dalykais. Todėl, nesant įtikinamų argumentų, EDAPP siūlo Europolui ir *Eurojust* suteikti tik po vieną prieigos vietą.

4.3. **Perspėjimų tarpusavio susiejimas**

Reglamento 26 straipsnyje ir sprendimo 46 straipsnyje numatoma, kad valstybės narės gali sukurti perspėjimų sąsajas pagal savo nacionalinės teisės aktus, siekdamos nustatyti dviejų ar daugiau perspėjimų santykį.

Nors perspėjimų sąsajos gali būti neabejotinai naudingos kontrolės tikslais (pavyzdžiui, arešto orderis automobilių vagiui gali būti susietas su pavogta transporto priemone), tokių sąsajų įvedimas yra labai tipiškas policijos tyrimo priemonės bruožas.

Perspėjimų tarpusavio susiejimas gali turėti didelį poveikį atitinkamo asmens teisėms, kadangi asmuo jau nebėra „vertinamas“ remiantis tik su juo susijusiais duomenimis, bet remiantis galimais jo ryšiais su kitais asmenimis. Tikėtina, kad į asmenis, kurių duomenys susiję su nusikaltėlių ar ieškomų asmenų duomenimis, bus žiūrima įtariau nei į kitus. Be to, tarpusavyje susiejant perspėjimus išplečiamos SIS tyrimo galios, nes tampa įmanoma registruoti tariamas nusikalstamas grupes ar tinklus (jeigu, pavyzdžiui, duomenys apie nelegalius imigrantus susieti su nelegalių prekiautojų duomenimis). Galiausiai, kadangi sąsajų nustatymas paliekamas nacionalinės teisės kompetencijai, gali atsitikti, kad sąsajas, laikomas nelegaliomis vienoje valstybėje narėje, gali nustatyti kita valstybė narė, taip įvesdama į sistemą „nelegalius“ duomenis.

[1] 2005 m. vasario 24 d. Tarybos sprendimas 2005/211/TVR dėl Šengeno informacinės sistemos kai kurių naujų funkcijų nustatymo, įskaitant kovos su terorizmu srityje, OL L 68/44, 2005 3 15.

2004 m. birželio 14 d. Tarybos išvadose dėl SIS II funkcinių reikalavimų nurodoma, kad kiekviena sąsaja privalo turėti aiškų veikimo reikalavimą, būti grindžiama aiškiai nustatytu santykiu ir atitikti proporcingumo principą. Be to, ji negali turėti įtakos prieigos teisėms. Bet kuriuo atveju, kadangi perspėjimų tarpusavio susiejimas yra tvarkymo operacija, ją vykdant privaloma laikytis nacionalinės teisės aktų, įgyvendinančių Direktyvą 95/46/EB ir/arba Konvenciją Nr. 108, nuostatų.

Pasiūlymuose kartojama, kad sąsajos negali keisti prieigos teisių (priešingu atveju tai suteiktų prieigą prie duomenų, kurių tvarkymas būtų neteisėtas pagal nacionalinę teisę, pažeidžiant direktyvos 6 straipsnį).

EDAPP pabrėžia siūlomo reglamento 26 straipsnio ir siūlomo sprendimo 46 straipsnio griežto aiškinimo svarbą: vienas būdų tai užtikrinti būtų aiškiai nurodyti, kad institucijoms, neturinčioms prieigos teisės prie tam tikrų duomenų kategorijų, ne tik negali būti suteikiama prieiga prie tų kategorijų sąsajų, bet jos net neturėtų žinoti, kad esama tokių sąsajų. Neturint prieigos teisės prie susietų duomenų, turi būti neįmanoma įsivaizduoti, kad yra jų sąsajų.

Be to, tam užtikrinti EDAPP pageidautų, kad su juo būtų konsultuojamasi dėl techninių priemonių.

4.4. **Perspėjimai dėl draudimo įvažiuoti**

4.4.1. *Įtraukimo pagrindas*

„Perspėjimų dėl draudimo įvažiuoti trečiųjų šalių piliečiams“ (Reglamento 15 straipsnis) naudojimas turi didelį poveikį asmenų laisvėms: asmuo, apie kurį pranešama pagal šią nuostatą, praranda teisę įvažiuoti į Šengeno erdvę kelerius metus. Iki šiol tai buvo dažniausiai naudojamas perspėjimas dėl visų asmenų, apie kuriuos buvo pranešta. Atsižvelgiant į šio perspėjimo pasekmes ir į susijusių asmenų skaičių, būtinas ypatingas atidumas jį formuluojant ir įgyvendinant. Nors tai taikytina ir kitiems perspėjimams, minėtam perspėjimui EDAPP skirs konkretų skyrių, kadangi jis kelia konkrečiais problemas dėl įtraukimo pagrindo.

Naujuoju perspėjimu dėl draudimo įvažiuoti esama padėtis pagerinama, tačiau nepakankamai, kadangi jis daugiausia grindžiamas dokumentais, kurie dar nebuvo priimti ar netgi pasiūlyti.

Patobulinamas tik duomenų įtraukimo pagrindo apibūdinimas, kuris nuo šiol yra tikslesnis. Dėl Šengeno konvencijoje pateiktos formuluotės asmenų, apie kuriuos pranešta pagal Konvencijos 96 straipsnį, skaičius valstybėse narėse labai skiriasi. Tuo klausimu Šengeno BPI atliko išsamų tyrimą [1] ir pateikė rekomendaciją, kad „politikos formuotojai turėtų apsvarstyti, ar nevertėtų suderinti perspėjimo davimo priežasčių skirtingose Šengeno valstybėse“.

Siūlomo 15 straipsnio formuluotė yra tikslesnė, o tai reikia palankiai įvertinti.

Be to, 15 straipsnio 2 dalyje taip pat išvardijami atvejai, kuriais negalima duoti perspėjimo apie asmenis, kadangi jie, pritaikius skirtingus statusus, teisėtai gyvena valstybės narės teritorijoje. Nors tokią išvadą galima buvo daryti remiantis galiojančia Šengeno konvencija, praktika parodė, kad šį mechanizmą valstybės narės taip pat taikė skirtingai. Todėl aiškumas yra teigiamas elementas.

Tačiau ši nuostata taip pat griežtai kritikuotina, kadangi ji daugiausia grindžiama dar neprimtu tekstu, t.y. direktyva „dėl grąžinimo“.

Priėmus SIS II pasiūlymus, (2005 m. rugsėjo 1 d.) Komisija pateikė pasiūlymą dėl „Direktyvos dėl neteisėtai gyvenančių trečiųjų šalių piliečių grąžinimo bendrų standartų ir procedūrų valstybėse narėse“, tačiau tol, kol teksto redakcija yra negalutinė, jo negalima laikyti tinkamu duomenų įtraukimo į sistemą pagrindu. Tai visų pirma pažeidžia ŽTPLK 8 straipsnį, kadangi kišimąsis į asmens privatų gyvenimą turėtų būti grindžiamas *inter alia* aiškiais ir prieinamais teisės aktais.

Todėl EDAPP ragina Komisiją išbraukti šią nuostatą arba jos formuluotę, remiantis galiojančiais teisės aktais, pakeisti taip, kad asmenys žinotų, kokių priemonių jų atžvilgiu institucijos iš tiesų gali imtis.

4.4.2. *Prieiga prie perspėjimų, duodamų pagal 15 straipsnį*

18 straipsnyje nustatyta, kurioms institucijoms ir kokiam tikslui suteikiama prieiga prie šių perspėjimų. 18 straipsnio 1 ir 2 dalyse nustatyta, kurioms institucijoms suteikiama prieiga prie perspėjimų, įtrauktų pagal direktyvą dėl grąžinimo. Galioja pirmiau minėtas komentaras.

[1] Šengeno bendros priežiūros institucijos ataskaita dėl 96 straipsnyje nustatytų perspėjimų naudojimo Šengeno informacinėje sistemoje patikrinimo, Briuselis, 2005 m. birželio 20 d.

Siūlomo reglamento 18 straipsnio 3 dalimi prieigos teisė suteikiama institucijoms, kurios pagal direktyvą, kurios pasiūlymas dar net nepateiktas, atsakingos už pabėgėlio statuso suteikimą. Atsižvelgdamas į tai, kad tekstas dar neegzistuoja, EDAPP privalo pakartoti pirmiau minėtas pastabas.

4.4.3. *Perspėjimų, duodamų pagal 15 straipsnį, saugojimo laikotarpis*

Pagal 20 straipsnį perspėjimo negalima saugoti ilgiau, nei sprendime (dėl grąžinimo ar išsiuntimo) nustatytą draudimo įvažiuoti laikotarpį. Tai neprieštarauja duomenų apsaugos taisyklėms. Be to, perspėjimas bus automatiškai ištrintas po penkerių metų, išskyrus atvejus, kai į SIS II įvedusios duomenis valstybės narės nusprendžia kitaip.

Nacionaliniu lygiu vykdoma tinkama priežiūra turėtų užtikrinti, kad saugojimo laikotarpis nebūtų automatiškai nepagrįstai pratęstas ir kad valstybės narės ištrintų duomenis nesuėjus penkerių metų terminui tuo atveju, jei draudimo įvažiuoti laikotarpis pasirodytų trumpesnis.

4.5. **Saugojimo laikotarpiai**

Nors saugojimo principas yra toks pat (paprastai perspėjimas turėtų būti ištrinamas iš SIS II iš karto po to, kai buvo imtasi perspėjimo sąlygotų veiksmų), pasiūlymais bus nustatyta, kad perspėjimų saugojimo laikotarpis yra iš esmės pratęsiamas.

Šengeno konvencijoje numatyta, kad būtinybė toliau saugoti duomenis turi būti peržiūrėta ne vėliau kaip po trejų metų nuo jų įvedimo (arba po vienerių metų, jei duomenys įvesti apdairaus sekimo tikslu). Naujuosiuose pasiūlymuose numatyta, kad imigracijos duomenys automatiškai ištrinami po penkerių metų, duomenys apie areštą, dingusius asmenis ir asmenis, ieškomus teisminio proceso tvarka — po 10 metų, o duomenys apie asmenis, kurie turi būti apdairiai sekami — po 3 metų (perspėjimą davusi valstybė narė turi galimybę prieštarauti automatiškam duomenų ištrynimui).

Nors iš esmės valstybės narės turės ištrinti duomenis, kai perspėjimo tikslas pasiektas, ilgiausias saugojimo laikotarpis smarkiai pailgėja (dažniausiai patrigubėja), o šio fakto Komisija niekaip nepagrindžia. Imigracijos duomenų atveju galima tik spėti, kad 5 metų trukmė susijusi su draudimo įvažiuoti laikotarpiu, numatytu direktyvos dėl grąžinimo projekte. Visais kitais atvejais EDAPP nėra žinoma nė viena motyvuota priežastis.

Galimas poveikis duomenų subjektams, apie kuriuos pranešama SIS, gali turėti didelių pasekmių atitinkamų asmenų gyvenime. Tai ypač neramina perspėjimų apie asmenis, kurie turi būti apdairiai sekami arba specialiai tikrinami atveju, kadangi šie perspėjimai gali būti išduodami įtarus.

EDAPP pageidautų, kad šis duomenų saugojimo laikotarpių pratęsimas būtų tvirtai pagrįstas. Jeigu nebus įtikinamų pagrindžiančių motyvų, jis siūlo palikti šiuo metu galiojančius laikotarpius, visų pirma to reikalaudamas perspėjimų apdairaus sekimo arba specialių patikrinimų tikslams atveju.

4.6. **Institucijų, atsakingų už transpoto priemonių registracijos liudijimų išdavimą, prieiga**

Pagrindinė problema siejama su ypač ginčytino teisinio pagrindo pasirinkimu. Komisijai nepavyko įtikinti, kad priemonei, kuri sudarytų galimybę administracinėms institucijoms naudotis SIS nusikalstamumo prevencijos ir kovos su nusikalstamumu tikslais (prekyba vogtomis transporto priemonėmis), turi būti naudojama pirmajam ramsčiui priklausanti „transporto“ teisinė bazė. Prieigos prie SIS II tvirto pagrindimo ir tvirtos teisinės bazės būtinybė buvo išsamiai apibūdinta šios nuomonės 4.2.2 punkte.

EDAPP remiasis pastabomis, kurias šiuo klausimu pateikė Šengeno BPI savo nuomonėje dėl siūlomos SIS II teisinės bazės. Visų pirma reikėtų atsižvelgti į Šengeno BPI siūlymą iš dalies pakeisti siūlomą sprendimą, į jį įtraukiant nuostatas dėl šios prieigos.

5. KOMISIJOS IR VALSTYBIŲ NARIŲ VAIDMUO

Norint, kad SIS II sistema ne tik sklandžiai veiktų, bet ir būtų užtikrinta jos priežiūra, būtina aiškiai apibūdinti ir paskirstyti atsakomybę šioje srityje. Priežiūros funkcijų padalijimas paaiškės apibūdinus atsakomybę, taigi šioje srityje būtinas visiškas aiškumas.

5.1. **Komisijos vaidmuo**

EDAPP palankiai vertina abiejų pasiūlymų III skyrius, kuriuose apibūdinamas Komisijos vaidmuo ir atsakomybė SIS II srityje („operatyvinio valdymo“ vaidmuo). VIS pasiūlyme tokio aiškumo trūko. Tačiau vien šio skyriaus nepakanka išsamiai apibūdinti Komisijos vaidmenį. Iš tiesų, kaip nagrinėjama šios nuomonės 9 skyriuje, Komisija taip pat dalyvauja sistemos įgyvendinime ir valdyme naudojant komitologijos procedūrą.

Duomenų apsaugos srityje Komisijai tenka VIS ir Eurodac sistemose jau pripažintas vaidmuo, t.y. atsakomybė už operatyvinį valdymą. Kartu su pagrindiniu vaidmeniu kuriant sistemą ir palaikant jos veikimą, šį jos vaidmenį reikėtų vertinti kaip *sui generis* duomenų valdytojo. Kaip jau minėta EDAPP nuomonėje dėl VIS, šis vaidmuo apima daugiau nei duomenų tvarkytojo, bet mažiau nei įprasto duomenų valdytojo funkcijas, kadangi Komisija neturi prieigos prie SIS II tvarkomų duomenų.

Atsižvelgiant į tai, kad kuriant SIS II bus naudojamos sudėtingos sistemos, iš kurių kelios priklauso nuo naujų technologijų, EDAPP primygtinai reikalauja padidinti Komisijos atsakomybę atnaujinant sistemas, tam pasitelkiant geriausias turimas technologijas, susijusias su saugumu ir duomenų apsauga.

Todėl pasiūlymų 12 straipsniai turėtų būti papildyti nuostata, kad Komisija turėtų reguliariai siūlyti diegti naujas technologijas, kurios šioje srityje būtų šiuolaikiškos, pagerintų duomenų apsaugos ir saugumo lygius bei sudarytų palankesnes sąlygas prieigą prie šių duomenų turinčioms nacionalinės valdžios institucijoms vykdyti užduotis.

5.2. **Valstybių narių vaidmuo**

Valstybių narių padėtis nėra visiškai aiški, kadangi yra gana sunku žinoti, kuriai (-ioms) institucijai (-oms) bus pavestos duomenų valdytojo (-ų) funkcijos.

Pasiūlymuose apibūdinamas SIS II nacionalinės įstaigos (siekiant užtikrinti, kad kompetentingos institucijos turėtų prieigą prie SIS II) ir SIRENE institucijų (siekiant užtikrinti, kad būtų keičiamasi visa papildoma informacija) vaidmuo. Valstybės narės taip pat turi užtikrinti jų NS („nacionalininės sistemos“) veikimą ir saugumą. Nėra aišku, ar ši pastaroji atsakomybė turi tekti vienai iš pirmiau minėtų institucijų. Bet kuriuo atveju, šioje srityje būtinas aiškumas.

Duomenų apsaugos srityje Komisija ir valstybės narės turėtų būti laikomos bendrais duomenų valdytojais, kiekvienai priskiriant konkrečią atsakomybę. Tik pripažinus šias papildomas užduotis, bus užtikrinta visų SIS II veiklos sričių priežiūra.

6. **DUOMENŲ SUBJEKTŲ TEISĖS**

6.1. **Informacija**

6.1.1. *Siūlomas reglamentas*

Siūlomo reglamento 28 straipsnyje numatyta duomenų subjekto teisė gauti informaciją, iš esmės laikantis Direktyvos 95/46 10 straipsnio. Palyginti su esama padėtimi, kai teisė gauti informaciją Konvencijoje nėra aiškiai įvardyta, šis postūmis yra sveikintinas. Tačiau dar vertėtų patobulinti šiuos dalykus.

Sąrašą vertėtų papildyti tam tikra informacija, kadangi tai užtikrintų, jog duomenų subjektui būtų taikomos tinkamos sąlygos ([1]). Ši informacija turėtų būti susijusi su duomenų saugojimo laikotarpiu, turima teise prašyti peržiūrėti arba apskųsti sprendimą išduoti perspėjimą (kai kuriais atvejais žr. siūlomo reglamento 15 straipsnio 3 dalį), galimybe gauti duomenų apsaugos institucijos paramą ir teisių gynimo priemonių egzistavimu.

Siūlomame reglamente nėra nuorodų į tai, kada informacija turėtų būti pateikta. Dėl šios priežasties duomenų subjektui gali tapti neįmanoma naudotis teisėmis. Tam, kad šios teisės būtų veiksmingos, reglamente turėtų būti tiksliai numatyta, kada ši informacija turėtų būti pateikta, atsžvelgiant į perspėjimą išdavusią instituciją.

Praktinis sprendimas būtų informacijos apie perspėjimą įtraukimas į sprendimą, kuris pirmiausia suteikia pagrindą perspėjimui: į teismo ar administracinį sprendimą, pagrįstą grėsme viešajai tvarkai (....) arba į sprendimą dėl grąžinimo ar į įsakymą dėl išsiuntimo, prie kurio pridedamas draudimas pakartotinai įvažiuoti. Ši nuostata turėtų būti įtraukta į reglamento 28 straipsnį.

6.1.2. *Siūlomas sprendimas*

Sprendimo 50 straipsnyje nustatyta, kad informacija suteikiama duomenų subjekto prašymu ir nurodomos galimos atsisakymo suteikti tokią informaciją priežastys. Atsižvelgiant į duomenų pobūdį ir jų tvarkymo sąlygas, aiškiai suprantama, kad yra nustatyti šios teisės apribojimai.

Tačiau teisei gauti informaciją neturėtų būti taikomas reikalavimas, kuris įpareigoja duomenų subjektą pateikti prašymą (tai iš esmės turėtų būti nustatoma apibrėžiant prašymo gauti prieigą sąvoką). Galima daryti prielaidą, kad būtinybė „prašyti“ informacijos buvo pagrįsta atvejais, kai duomenų subjektas negali būti informuojamas dėl to, kad nėra nustatyta jo buvimo vieta.

Šis klausimas būtų išspręstas geriau, jei tais atvejais, kai perduoti informacijos neįmanoma arba kai jos perdavimas pareikalautų neproporcingų pastangų, būtų nustatyta teisės gauti informaciją išimtis. Todėl sprendimo 50 straipsnį vertėtų iš dalies pakeisti.

([1]) Taip pat žr. EDAPP nuomonės dėl vizų informacinės sistemos sukūrimo 3.10.1 punktą.

Šis sprendimo būdas taip pat neprieštarautų pamatinio sprendimo dėl duomenų apsaugos trečiojo ramsčio srityje projekto taikymui.

6.2. **Prieiga**

Siūlomuose reglamente ir sprendime nustatyti atsakymo į prašymus gauti prieigą pateikimo terminai, o tai yra teigiamas postūmis. Tačiau atsižvelgiant į tai, kad naudojimosi prieigos teise tvarka yra apibrėžta nacionaliniu lygiu, galima kelti klausimą, kaip su esama tvarka galima sieti pasiūlymuose nustatytus terminų atidėjimus, visų pirma tais atvejais, kai valstybių narių nustatyti atsakymo į prašymą gauti prieigą terminai yra trumpesni. Turėtų būti aiškiai įvardyta, kad turėtų būti taikomi duomenų subjektui palankiausi terminai.

6.2.1. *Siūlomas reglamentas*

Verta pažymėti, kad galiojančioje Šengeno konvencijoje numatyti prieigos teisės apribojimai („atsisakoma suteikti, jei tai gali pakenkti teisėtos užduoties, susijusios su perspėjimu, atlikimui arba siekiant apsaugoti trečiųjų šalių teises ir laisves“) siūlome reglamente nenustatyti.

Tačiau taip įvyko greičiausiai dėl to, kad yra taikoma Direktyva 95/46/EB, kurioje numatyta (13 straipsnyje) galimybė taikyti nacionalinės teisės aktuose numatytas išimtis. Bet kuriuo atveju vertėtų pažymėti, kad 13 straipsnio naudojimas nacionalinės teisės aktuose ribojant teisę gauti prieigą negali prieštarauti EŽTPLK 8 straipsniui, taigi, naudojamas tik ribotais atvejais.

6.2.2. *Siūlomas sprendimas*

Siūlomame sprendime, kaip ir Šengeno konvencijoje, numatytas prieigos teisės apribojimas. Siūlomame pamatiniame sprendime iš esmės numatyti tie patys prieigos teisės apribojimai; todėl priėmus šį dokumentą, nebūtų padaryta didesnių skirtumų šioje srityje.

Kadangi keliose valstybėse narėse prieiga prie teisėsaugos informacijos yra „netiesioginė“ (t.y., šia teise naudojamasi per nacionalinę duomenų apsaugos instituciją), vertėtų numatyti prievolę duomenų apsaugos institucijoms aktyviai bendradarbiauti prieigos teisės naudojimosi srityje.

6.3. **Teisė peržiūrėti arba apskųsti sprendimą išduoti perspėjimą**

Tais atvejais, kai sprendimą išduoti perspėjimą priima administracinės valdžios institucija, reglamento 15 straipsnio 3 dalyje numatyta teisė dėl tokio sprendimo peržiūros ar apskundimo kreiptis į teisminę instituciją. Palyginti su galiojančia Šengeno konvencija, ši papildoma nuostata sveikintina.

Tai pabrėžia būtinybę išsamiai ir laiku informuoti duomenų subjektą, kaip nurodyta pirmiau minėtame 6.1 punkte: jei duomenų subjektas nebus informuojamas, ši nauja teisė bus tik teorinė.

6.4. **Teisės gynimo būdai**

Siūlomo reglamento 30 straipsnyje ir siūlomo sprendimo 52 straipsnyje numatyta teisė pareikšti ieškinį arba paduoti skundą bet kurios valstybės narės teismams, jeigu duomenų subjektui atsisakoma suteikti prieigos teisę, nepataisomi ar neištrinami duomenys ir atsisakoma suteikti teisę gauti informaciją arba teisę į nuostolių atlyginimą.

Formuluotė („visi asmenys bet kurios valstybės narės teritorijoje“) reiškia, kad norėdamas paduoti ieškinį teismui, ieškovas fiziškai privalo būti toje teritorijoje. Šis teritorinis apribojimas nepateisinamas, ir dėl jo teisių gynimo priemonės galėtų būti neveiksmingos, kadangi labai dažnai tikėtina, kad ieškovas pateiks ieškinį būtent dėl to, kad jam nesuteikiama teisė įvažiuoti į Šengeno teritoriją. Be to, atsižvelgiant į tai, kad direktyva yra *lex generalis*, siūlomame reglamente būtina atsižvelgti į jos 22 straipsnį; jame nustatyta, kad „kiekvienas asmuo“, neatsižvelgiant į jo gyvenamąją vietą, turi teisę į teisminę gynybą. Siūlomame pamatiniame sprendime taip pat nėra teritorinio apribojimo nuostatos. EDAPP siūlo 30 straipsnyje ir 52 straipsnyje atsisakyti teritorinio apribojimo nuostatos.

7. PRIEŽIŪRA

7.1. **Įvadinė pastaba: atsakomybės pasidalijimas**

Pasiūlymuose padalijamos nacionalinių priežiūros institucijų ([1]) ir EDAPP priežiūros funkcijos kiekvienam pagal pavesto darbo sritis. Tai atitinka pasiūlymuose išreikštą požiūrį į taikytiną teisę ir su SIS II veikimu bei naudojimu susijusius įsipareigojimus ir į veiksmingos priežiūros būtinybę.

Todėl EDAPP palankiai vertina šį siūlomo reglamento 31 straipsnyje ir siūlomo sprendimo 53 straipsnyje nustatytą požiūrį. Tačiau siekiant geriau suvokti ir išaiškinti atitinkamus uždavinius, EDAPP siūlo kiekvieną straipsnį padalyti į kelias nuostatas, kurių kiekviena būtų skirta tam tikram priežiūros lygiui, kaip kad buvo tinkamai padaryta pasiūlyme dėl VIS.

([1]) Įtraukiamos Europolo ir *Eurojust* priežiūros institucijos, tačiau mažesniu mastu.

7.2. **Nacionalinių duomenų apsaugos institucijų vykdoma priežiūra**

Pagal siūlomo reglamento 31 straipsnį ir siūlomo sprendimo 53 straipsnį kiekviena valstybė narė privalo užtikrinti, kad nepriklausoma institucija vykdytų SIS II asmens duomenų tvarkymo teisėtumo stebėseną.

Be to, siūlomo sprendimo 53 straipsnyje numatyta konkretaus asmens teisė prašyti priežiūros institucijos patikrinti, ar duomenys apie jį tvarkomi teisėtai. Atsižvelgiant į tai, kad direktyva taikoma kaip *lex generalis*, panaši nuostata į siūlomą reglamentą nebuvo įtraukta. Todėl reikia manyti, kad nacionalinės duomenų apsaugos institucijos SIS II atžvilgiu gali naudotis visais joms pagal Direktyvos 95/46/EB 28 straipsnį suteiktais įgaliojimais, įskaitant duomenų tvarkymo teisėtumo tikrinimą. Reglamento 31 straipsnio 1 dalyje patikslinama jų užduotis, tačiau tai negali reikšti jų įgaliojimų apribojimo. Siūlomo reglamento tekste šių įgaliojimų pripažinimas turėtų būti aiškesnis.

Atsižvelgiant į tai, kad siūlomo sprendimo *lex generalis* yra kitoks, jame pripažįstamos platesnės nacionalinių priežiūros institucijų pareigos. Tačiau padėtis, kai priežiūros institucijos turėtų skirtingas užduotis ir įgaliojimus pagal tvarkomų duomenų kategoriją, nėra tinkama ir ją praktiškai valdyti yra labai sunku. Todėl pripažįstant duomenų apsaugos institucijoms tuos pačius įgaliojimus pačiame siūlomo sprendimo tekste arba darant nuorodą į kitą *lex generalis* (visų pirma pamatinį sprendimą dėl duomenų apsaugos trečiojo ramsčio srityje), vertėtų vengti suteikti šioms institucijoms daugiau įgaliojimų.

7.3. **EDAPP vykdoma priežiūra**

EDAPP kontroliuoja, kad Komisijos duomenų tvarkymo veikla būtų vykdoma pagal pasiūlymus. Taip pat EDAPP turėtų būti suteikta galimybė naudotis visais jam pagal Reglamentą 45/2001 suteiktais įgaliojimais, tačiau atsižvelgiant į ribotus Komisijos įgaliojimus pačių duomenų atžvilgiu.

Verta pažymėti, kad pagal Reglamento 45/2001 46 straipsnio f punktą EDAPP „turi bendradarbiauti su nacionalinėmis priežiūros institucijomis tiek, kiek tai būtina jų atitinkamoms pareigoms atlikti“. Šį bendradarbiavimą su valstybėmis narėmis SIS II priežiūros srityje lemia ne tik pasiūlymai, bet ir Reglamentas 45/2001.

7.4. **Bendra priežiūra**

Pasiūlymuose taip pat pripažįstama būtinybė derinti skirtingų dalyvaujančių institucijų priežiūros veiklą. Siūlomo reglamento 31 straipsnyje ir siūlomo sprendimo 53 straipsnyje numatyta, kad „nacionalinės priežiūros institucijos ir Europos duomenų apsaugos priežiūros pareigūnas aktyviai tarpusavyje bendradarbiauja. Europos duomenų apsaugos priežiūros pareigūnas ne rečiau kaip kartą per metus šiuo tikslu šaukia posėdį.“

EDAPP palankiai vertina šį pasiūlymą, kuriame iš esmės numatyti visi būtini dalykai bendradarbiavimui, kuris institucijoms, atsakingoms už priežiūrą nacionaliniu ir Europos lygiu, iš tiesų svarbus, užtikrinti. Reikėtų pabrėžti, kad pasiūlymuose numatyta sušaukti posėdį ne rečiau kaip kartą per metus, tačiau šis posėdžių skaičius yra minimalus.

Tačiau vertėtų šiek tiek aiškiau išdėstyti šias minėto veiksmų derinimo turinį apibrėžiančias nuostatas (siūlomo reglamento 31 straipsnis ir siūlomo sprendimo 53 straipsnis). Egzistuojanti bendros priežiūros institucija turi įgaliojimus nagrinėti Konvencijos aiškinimo ar taikymo sunkumus, nagrinėti problemas, kurios gali kilti vykdant nepriklausomą priežiūrą arba naudojantis prieigos teise ir parengti suderintus pasiūlymus dėl bendrų esamų problemų sprendimo būdų.

Naujais pasiūlymais negalima sumažinti esamo bendros priežiūros masto. Jeigu akivaizdu, kad duomenų apsaugos institucijos SIS II atžvilgiu gali naudotis visais pagal direktyvą joms suteiktais priežiūros įgaliojimais, šių institucijų bendradarbiavimas gali apimti įvairius SIS II priežiūros aspektus, įskaitant pagal Šengeno konvencijos 115 straipsnį nustatytas egzistuojančios bendros priežiūros institucijos užduotis.

Tačiau siekiant visiško aiškumo, vertėtų tai aiškiai dar kartą įtvirtinti pasiūlymuose.

8. SAUGUMAS

SIS II optimalaus saugumo lygio valdymas ir jo užtikrinimas yra vienas pagrindinių reikalavimų tinkamai duomenų bazėje saugomų asmens duomenų apsaugai užtikrinti. Siekiant šio reikiamo apsaugos lygio, turi būti įgyvendintos tinkamos apsaugos priemonės, skirtos susidoroti su galimais pavojais, susijusiais su sistemos infrastruktūra ir su sistemoje dalyvaujančiais asmenimis. Šiuo metu šis klausimas yra nagrinėjamas įvairiose pasiūlymo dalyse ir turėtų būti šiek tiek patobulintas.

Pasiūlymo 10 ir 13 straipsniuose numatytos įvairios duomenų saugumo priemonės bei nurodyti netinkamo naudojimo būdai, kuriems turi būti užkirstas kelias. EDAPP palankiai vertina tai, kad į šiuos straipsnius buvo įtrauktos nuostatos dėl sistemingos saugumo priemonių (savi)kontrolės.

Tačiau siūlomo sprendimo 59 straipsnyje ir siūlomo reglamento 34 straipsnyje, kuriuose numatytos nuostatos dėl stebėsenos ir vertinimo, turėtų būti nagrinėjami ne tik išvesties duomenų, ekonominio efektyvumo ir paslaugų kokybės aspektai, bet ir atitiktis teisiniams reikalavimams, visų pirma duomenų apsaugos srityje. Todėl EDAPP rekomenduoja išplėsti šių straipsnių taikymo sritį taip, kad ji apimtų stebėseną bei pranešimų apie duomenų tvarkymo teisėtumą teikimą.

Be to, papildant siūlomo sprendimo 10 straipsnio 1 dalies f punktą arba 18 straipsnį ir siūlomo reglamento 17 straipsnį dėl tinkamai įgalioto personalo, turinčio prieigą prie duomenų, reikėtų įterpti tai, kad valstybės narės (įskaitant Europolą ir *Eurojust*) turėtų užtikrinti, kad būtų prieinamos tikslios vartotojų kategorijos (kurios būtų tikrinimą vykdančių nacionalinių priežiūros institucijų žinioje). Be šių vartotojų kategorijų valstybės narės turėtų sudaryti ir nuolat atnaujinti išsamų vartotojų tapatybių sąrašą. Tas pats *mutatis mutandis* taikoma Komisijai.

Šios saugumo priemonės papildomos stebėsenos ir organizacinėmis apsaugos priemonėmis. Pasiūlymų 14 straipsniuose apibūdintos sąlygos ir tikslai, kuriems turi būti registruojami visų duomenų tvarkymo operacijų įrašai. Tokie įrašai saugomi ne tik siekiant kontroliuoti duomenų apsaugą bei užtikrinti duomenų saugumą, bet taip pat ir sustiprinti reguliarią SIS II savikontrolę, kurios reikalaujama pagal 10 straipsnį. Savikontrolės ataskaitos padės priežiūros institucijoms veiksmingai vykdyti užduotis, kadangi šios institucijos turės galimybę nustatyti silpniausias vietas ir sutelkti į jas pagrindinį dėmesį atliekant auditą.

Kaip jau buvo pirmiau nurodyta šioje nuomonėje, didesnį prieigos prie sistemos vietų skaičių būtina rūpestingai pagrįsti, kadangi dėl jo automatiškai padidėtų netinkamo naudojimo rizika. Todėl pasiūlymų 4 straipsnio 1 dalies b punktuose turėtų būti reikalaujama konkrečiai įrodyti antros prieigos vietos poreikį.

Pasiūlymuose aiškiai nenurodyta, kam reikalingos centrinės sistemos nacionalinės kopijos; jie kelia didelį susirūpinimą bendru pavojaus ir sistemos saugumo lygiu, pavyzdžiui:

— kopijų padauginimas kelia netinkamo naudojimo riziką (ypač atsižvelgiant į naujų duomenų, pavyzdžiui, biometrinių duomenų, atsiradimą);

— su šiomis kopijomis siejami duomenys nėra tinkamai apibrėžti;

— 9 straipsnyje nustatyti tikslumo, kokybės ir prieinamumo reikalavimai kelia didelių techninių sunkumų ir todėl padidina sąnaudas, atsižvelgiant į turimų technologijų šiuolaikiškumą;

— dėl nacionalinės valdžios institucijų vykdomos šių kopijų kontrolės prireiks papildomų žmogiškųjų išteklių ir finansinių lėšų, kurių ne visada galima surasti.

Atsižvelgdamas į susijusią riziką, EDAPP nėra įsitikinęs nei nacionalinių kopijų naudojimo būtinybe (atsižvelgiant į turimas technologijas), nei tokio naudojimo pridėtine verte. Jis rekomenduoja atsisakyti galimybės valstybėms narėms naudoti nacionalines kopijas.

Tačiau jei nacionalines kopijas parengti būtina, EDAPP primena, kad jas naudojant nacionaliniu lygiu turi būti taikomas griežtas tikslo ribojimo principas. Be to, nacionalinė kopija gali būti paieškoma tik per centrinę duomenų bazę.

Asmens duomenų tvarkymo operacijos teisėtumas grindžiamas griežtu duomenų saugumo ir duomenų vientisumo principų laikymusi. EDAPP veiksmingai vykdys šių procesų stebėseną, jei jam bus suteikta galimybė stebėti ne tik duomenų saugumą, bet ir jų vientisumą analizuojant turimus registracijos žurnalus. Todėl 14 straipsnio 6 dalis turėtų būti papildyta žodžiais „duomenų vientisumą“.

9. **KOMITOLOGIJA**

Pasiūlymuose numatyta, kad kai kuriais atvejais, kai SIS II įgyvendinimui ir valdymui būtina priimti technologinio pobūdžio sprendimus, taikomos komitologijos procedūros. Kaip jau dėl panašių priežasčių buvo nurodyta nuomonėje dėl VIS, šie sprendimai turės didelį poveikį tinkamam tikslo ir proporcingumo principo įgyvendinimui.

EDAPP pataria didelį poveikį duomenų apsaugai turinčius sprendimus, pavyzdžiui, dėl prieigos prie duomenų arba jų įvedimo, keitimosi papildoma informacija, duomenų kokybės ir perspėjimų suderinamumo, nacionalinių kopijų techninės atitikties, ir t.t., priimti reglamento arba sprendimo forma, pageidautina, numatant bendro sprendimo procedūrą ([1]).

([1]) Taip pat žiūrėti EDAPP nuomonės dėl Vizų informacinės sistemos 3.12 punktą ir 2005 m. rugsėjo 26 d. pateiktos EDAPP nuomonės dėl pasiūlymo dėl Direktyvos dėl duomenų, tvarkomų teikiant viešąsias elektroninių ryšių paslaugas, saugojimo 60 punktą.

Visais kitais duomenų apsaugai poveikį turinčiais atvejais EDAPP turėtų būti suteikiama galimybė patarti dėl šių komitetų pasirinkimo.

EDAPP patariamasis vaidmuo turėtų būti įtrauktas į sprendimo 60 ir 61 straipsnius bei reglamento 35 straipsnį.

Konkretesniu perspėjimų susiejimo techninių taisyklių atveju (reglamento 26 straipsnis ir sprendimo 46 straipsnis) turi būti išaiškinta skirtingo komitologijos pobūdžio (patariamasis pobūdis sprendimo atveju ir reglamentavimo pobūdis reglamento atveju) būtinybė.

10. **SĄVEIKA**

Kadangi Komisija vis dar nėra parengusi komunikato dėl naujų ES sistemų sąveikos, sunku tinkamai apskaičiuoti numatytos, bet dar neapibrėžtos sinergijos pridėtinę vertę.

Atsižvelgdamas į tai, EDAPP taip pat norėtų paminėti 2004 m. kovo 25 d. Tarybos deklaraciją dėl kovos su terorizmu, kurioje Komisijos prašoma pateikti pasiūlymus, siekiant sustiprinti informacinių sistemų (SIS, VIS ir Eurodac) sąveiką ir sinergiją. Jis taip pat norėtų paminėti vykstančias diskusijas dėl to, kuriai institucijai ateityje galėtų būti patikėtas skirtingų didelės apimties sistemų valdymas (žr. taip pat šios nuomonės 3.8 punktą).

Savo nuomonėje dėl Vizų informacinės sistemos EDAPP jau yra teigęs, kad tam, kad didelės apimties IT sistemos, pavyzdžiui, SIS II, būtų veiksmingos, lemiamas ir esminis reikalavimas būtų išlaikyti jų sąveiką. Ji suteikia galimybę nuosekliai mažinti bendras sąnaudas ir išvengti įprasto nevienalyčių elementų perteklumo.

— Sąveika taip pat gali padėti siekti tikslo išlaikyti aukštą saugumo lygį valstybių narių teritorijoje, kurioje nėra vidinių sienų kontrolės, visoms šios politikos sudedamosioms dalis taikant tą patį procedūrinį standartą. Tačiau svarbu išskirti du sąveikos lygmenis:

  — ES valstybių narių sąveika yra labai pageidautina; iš tiesų, vienos valstybės narės institucijų siunčiami perspėjimai turi būti sąveikūs su kitos valstybės narės institucijų siunčiamais perspėjimais.

  — Skirtingiems tikslams sukurtų sistemų tarpusavio sąveika arba sąveika su trečiosios šalies sistemomis kelia daugiau abejonių.

Be kitų galimų apsaugos priemonių, naudojamų apriboti sistemos paskirtį ir išvengti veiklos sutrikimų, prisidėti prie šio apribojimo galima taikant skirtingus technologinius standartus. Be to, kiekviena dviejų skirtingų sistemų sąveikos forma turėtų būti išsamiai pagrindžiama dokumentais. Sąveika niekada neturėtų sukurti sąlygų, kai valdžios institucija, kuriai nesuteikta prieigos prie tam tikrų duomenų teisė arba teisė juos naudoti, gali įgyti šią prieigą per kitą informacinę sistemą. Tiek, kiek tai galima numatyti susipažinus su pasiūlymais, atrodytų, kad, pavyzdžiui, automatinio pirštų anspaudų identifikavimo sistema (AFIS) pirmaisiais SIS II gyvavimo metais neegzistuos; pateikiama tik nuoroda į būsimą biometrinių duomenų paieškos mechanizmą. Numačius scenarijų, pagal kurį būtų naudojamos kitų ES sistemų AFIS, tai turėtų būti aiškiai pagrįsta dokumentais, numatant tokiai sinergijai būtinas apsaugos priemones.

EDAPP dar kartą nori pabrėžti, kad sistemų sąveika negali būti įgyvendinama pažeidžiant tikslo ribojimo principą ir tai, kad jam turėtų būti pateikiami visi pasiūlymai šiuo klausimu.

11. **IŠVADŲ SANTRAUKA**

11.1. **Bendri klausimai**

1. EDAPP palankiai vertina keletą teigiamų šių pasiūlymų aspektų, kurie tam tikrais klausimais pagerina esamą padėtį. Jis pripažįsta, kad iš esmės duomenų apsaugos nuostatos buvo parengtos atidžiai.

2. EDAPP pabrėžia, kad naujoji teisinė tvarka, nesvarbu, kokia sudėtinga bebūtų, turėtų:

   — užtikrinti aukštą duomenų apsaugos lygį,

   — būti nuspėjama piliečiams ir institucijoms, kurios keičiasi duomenimis,

   — ją taikant būti suderinama su dviem skirtingais kontekstais (pirmuoju ar trečiuoju ramsčiais).

3. Be to, SIS II papildant naujais elementais, padidinančiais jos galimą poveikį atskirų asmenų gyvenimui, turėtų būti nustatomos griežtesnės apsaugos priemonės, kurios apibūdinamos nuomonėje. Visų pirma:

— prieigos prie SIS II duomenų negalima suteikti naujoms institucijoms, jeigu tam nėra rimto pagrindo. Prieiga prie sistemos turėtų būti kuo labiau ribojama tiek prieinamų duomenų, tiek asmenų, įgaliotų tai daryti, atžvilgiu.

— Perspėjimų sąveika net netiesiogiai niekada negali pakeisti prieigos teisių.

— Dar nepriimtų teisės aktų negalima laikyti tinkamu duomenų įtraukimo į SIS II pagrindu (perspėjimai dėl draudimo įvažiuoti).

— Institucijų, atsakingų už transporto priemonių registracijos liudijimų išdavimą, prieigos teisinė bazė turėtų būti išnagrinėta iš naujo, kadangi iš esmės ji skirta kovai su nusikalstamumu.

— EDAPP pripažįsta, kad biometrinių duomenų naudojimas galėtų pagerinti sistemos veikimą ir padėti nukentėjusiems nuo tapatybės vagystės. Tačiau neatrodo, kad šio įtraukimo poveikis būtų pakankamai apgalvotas, ir šių duomenų patikimumas atrodo perdėtas.

11.2. **Konkrečios pastabos**

1. EDAPP palankiai vertina tai, kad Komisija pripažįsta, jog Reglamentas 45/2001 taikomas visoms Komisijos vykdomos duomenų tvarkymo veiklos SIS II sistemoje rūšims ir kad jis padės užtikrinti, jog taisyklės dėl asmenų pagrindinių teisių ir laisvių, susijusių su asmens duomenų tvarkymu, apsaugos būtų taikomos nuosekliai ir vienodai.

2. Siekiant užtikrinti griežto ribojimo principo nacionaliniu lygiu taikymą, EDAPP siūlo SIS II pasiūlymus (visų pirma siūlomo reglamento 21 straipsnį ir siūlomo sprendimo 40 straipsnį) papildyti į Šengeno konvencijos 102 straipsnio 4 dalyje apibrėžtos nuostatos poveikį panašia nuostata, ribojančia valstybių narių galimybę naudoti SIS II dokumentuose nenumatytus duomenis.

3. Griežti reikalavimai turėtų būti taikomi suteikiant bet kuriai institucijai prieigą prie SIS II duomenų:

— Prieiga turi atitikti bendrą SIS II tikslą ir teisinę bazę.

— Būtina įrodyti, kad prieig prie SIS II duomenų YRA REIKALINGA.

— Turi būti aiškiai apibrėžta, kokiu tikslu duomenys bus naudojimi ir apribotos jų naudojimo galimybės.

— Prieigos suteikimo sąlygos turi būti gerai apibrėžtos ir apribotos. Visų pirma turėtų būti nuolat atnaujinamas asmenų, turinčių prieigos teisę prie SIS II duomenų, sąrašas, įskaitant Europolą ir *Eurojust*.

— Tai, kad šioms institucijoms suteikta prieiga prie SIS II duomenų niekada negali būti laikoma pagrindu įvesti duomenis į sistemą arba juos ten laikyti, jeigu jie nėra naudingi konkrečiam perspėjimui, kurio dalimi jie yra.

— Duomenų saugojimo laikotarpio pratęsti negalima, išskyrus atvejus, kai tai būtina tam tikslui, kuriam duomenys buvo įvesti.

4. Konkrečiais Europolo ir *Eurojust* atvejais EDAPP primygtinai reikalauja, kad Komisija apribotų užduotis, kurioms atlikti būtų pagrįsta prieiga. Be to, Europolo ir *Eurojust* prieiga prie duomenų apie asmenis, kurių pavardės jau yra įtrauktos į jų dokumentų bylas, turėtų būti apribota. Taip pat siūloma Europolui ir *Eurojust* suteikti tik po vieną prieigos vietą.

5. Perspėjimų dėl draudimo įvažiuoti atveju nuostatos, kurios grindžiamos dar nepriimtais teisės aktais, turėtų būti išbrauktos arba jų formuluotė, remiantis galiojančiais teisės aktais, turėtų būti pakeista taip, kad asmenys žinotų, kokių priemonių jų atžvilgiu institucijos iš tiesų gali imtis.

6. Duomenų saugojimo laikotarpiai buvo pratęsti nepateikus tam jokio rimto pagrindo. Jeigu nebus įtikinamų pagrindžiančių motyvų, turėtų būti paliktas esamas saugojimo laikotarpių terminas, visų pirma perspėjimų apdairaus sekimo arba specialių patikrinimų tikslais atveju.

7. Komisijai tenka vienos iš atsakingųjų už operatyvinį valdymą vaidmuo. Kartu su jos pagrindiniu vaidmeniu kuriant sistemą ir palaikant jos veikimą, šį jos vaidmenį reikėtų vertinti kaip *sui generis* duomenų valdytojo. Šis vaidmuo apima daugiau nei duomenų tvarkytojo, bet mažiau nei įprasto duomenų valdytojo funkcijas, kadangi Komisija neturi prieigos prie SIS II tvarkomų duomenų.

   Atsižvelgiant į minėtą vaidmenį, abiejų pasiūlymų 12 straipsniai turėtų būti papildyti nuostata, kad Komisija turėtų reguliariai siūlyti diegti naujas technologijas, kurios šioje srityje būtų šiuolaikiškos ir pagerintų duomenų apsaugos ir saugumo lygius.

8. Valstybių narių vaidmens atveju būtina patikslinti duomenų valdytojo funkcijas turinčias institucijas.

9. Dėl duomenų subjekto informavimo:

   — Siūlomame reglamente sąrašas turėtų būti papildytas tam tikra informacija: duomenų saugojimo laikotarpiu, turima teise prašyti peržiūrėti arba apskųsti sprendimą išduoti perspėjimą, galimybe gauti duomenų apsaugos institucijos paramą ir teisių gynimo priemonių egzistavimu.

   Be to, informacijos pateikimo momentu pirmiausia būtina sprendime, kuris yra perspėjimo pagrindas, pateikti informaciją apie perspėjimą.

   — Siūlomo sprendimo 50 straipsnį reikėtų iš dalies pakeisti, kad duomenų subjektui nereikėtų pateikti prašymo gauti informaciją.

10. Atsakymo į prašymą gauti prieigą terminų atveju palankiai vertinama tai, kad pasiūlymuose yra nustatyti terminai. Tais atvejais, kad terminai nustatyti ir nacionalinės teisės aktuose, turėtų būti aiškiai įvardyta, kad turėtų būti taikomi tie terminai, kurie duomenų subjektui yra palankiausi.

    Be to, būtų naudinga numatyti duomenų apsaugos institucijoms prievolę aktyviai bendradarbiauti naudojantis prieigos teise.

11. Teisių gynimo priemonių atveju EDAPP siūlo atsisakyti teritorinio apribojimo nuostatos 30 ir 52 straipsniuose.

12. Dėl nacionalinių duomenų apsaugos institucijų įgaliojimų:

    — reglamente: reikia manyti, kad jos SIS II atžvilgiu gali naudotis visais joms pagal Direktyvos 95/46/EB 28 straipsnį suteiktais įgaliojimais; ši nuostata siūlomo reglamento tekste turėtų būti patikslinta.

    — Siūlomame sprendime: priežiūros institucijoms turėtų būti pripažinti tie patys įgaliojimai, kurie yra numatyti reglamente/ direktyvoje.

13. Dėl EDAPP įgaliojimų: EDAPP turėtų turėti galimybę naudotis visais jam pagal Reglamentą 45/2001 suteiktais įgaliojimais, tačiau atsižvelgiant į ribotus Komisijos įgaliojimus pačių duomenų atžvilgiu.

14. Dėl suderintos priežiūros: pasiūlymuose taip pat pripažįstama būtinybė derinti skirtingų dalyvaujančių institucijų priežiūros veiklą. EDAPP palankiai vertina tai, kad pasiūlymuose iš esmės numatyti visi būtini dalykai institucijų, atsakingų už priežiūrą nacionaliniu ir Europos lygiu, bendradarbiavimui užtikrinti. Tačiau vertėtų šiek tiek aiškiau išdėstyti šias minėto veiksmų derinimo turinį apibrėžiančias nuostatas (siūlomo reglamento 31 straipsį ir siūlomo sprendimo 53 straipsnį).

15. Pasiūlymo 10 ir 13 straipsniuose numatytos įvairios duomenų saugumo priemonės; palankiai vertinama tai, kad buvo įtrauktos nuostatos dėl sistemingos saugumo priemonių (savi)kontrolės.

    — Tačiau siūlomo sprendimo 59 straipsnyje ir siūlomo reglamento 34 straipsnyje, kuriuose numatytos nuostatos dėl stebėsenos ir vertinimo, turėtų būti nagrinėjami ne tik išvesties duomenų, ekonominio efektyvumo ir paslaugų kokybės aspektai, bet ir atitiktis teisiniams reikalavimams, visų pirma duomenų apsaugos srityje. Šios nuostatos turėtų būti atitinkamai iš dalies pakeistos.

    — Be to, papildant siūlomo sprendimo 10 straipsnio 1 dalies f punktą arba 18 straipsnį ir siūlomo reglamento 17 straipsnį, reikėtų įterpti tai, kad valstybės narės, Europolas ir *Eurojust* turėtų užtikrinti, kad būtų prieinamos tikslios vartotojų kategorijos (kurios būtų tikrinimą vykdančių nacionalinių priežiūros institucijų žinioje). Be šių vartotojų kategorijų valstybės narės turi sudaryti ir nuolat atnaujinti išsamų vartotojų tapatybių sąrašą. Tas pats taikoma Komisijai.

    — Asmens duomenų tvarkymo operacijos teisėtumas grindžiamas griežtu duomenų saugumo ir duomenų vientisumo principų laikymusi. EDAPP turėtų būti suteikta galimybė stebėti ne tik duomenų saugumą, bet ir jų vientisumą, analizuojant turimus registracijos žurnalus. Todėl 14 straipsnio 6 dalis turėtų būti papildyta žodžiais „duomenų vientisumą“.

16. Nacionalinių kopijų naudojimas gali sukelti daug papildomos rizikos. EDAPP nėra įsitikinęs nei nacionalinių kopijų naudojimo būtinybe (atsižvelgiant į turimas technologijas), nei tokio naudojimo pridėtine verte. Jis rekomenduoja vengti valstybėms narėms suteikti galimybę naudoti nacionalines kopijas arba bent jau ją griežtai apriboti. Tačiau jei nacionalines kopijas parengti būtina, jas naudojant nacionaliniu lygiu turi būti taikomas griežtas tikslo ribojimo principas. Be to, nacionalinė kopija gali būti paieškoma tik per centrinę duomenų bazę.

17. Dėl komitologijos: didelį poveikį duomenų apsaugai turintys sprendimai turėtų būti priimami reglamento arba sprendimo forma, pageidautina, numatant bendro sprendimo procedūrą. Tais atvejais, kai iš tiesų naudojama komitologijos procedūra, EDAPP patariamasis vaidmuo turėtų būti įtrauktas į sprendimo 60 ir 61 straipsnius bei reglamento 35 straipsnį.

18. Sistemų sąveika negali būti įgyvendinama pažeidžiant tikslo ribojimo principą; EDAPP reikėtų pateikti visus pasiūlymus šiuo klausimu.

Priimta Briuselyje, 2005 m. spalio 19 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas