

I

(Beslutninger og resolutioner, henstillinger og udtalelser)

UDTALELSER

DEN EUROPÆISKE TILSYNSFØRENDE FOR
DATABESKYTTELSE**Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om udkastet til forslag til Rådets rammeafgørelse om anvendelse af passagerlister (PNR-oplysninger) med henblik på retshåndhævelse**

(2008/C 110/01)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ⁽¹⁾,

som henviser til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger ⁽²⁾, særlig artikel 41,

som henviser til Kommissionens anmodning om udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001, der blev modtaget den 13. november 2007,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

Høring af den tilsynsførende

1. Kommissionen har sendt den tilsynsførende et udkast til et forslag til Rådets rammeafgørelse om anvendelse af passagerlister (PNR-oplysninger) med henblik på retshåndhævelse (i det følgende benævnt »forslaget«) til høring i

overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001.

2. Forslaget omhandler behandling af PNR-oplysninger i EU og hænger tæt sammen med andre ordninger for indsamling og anvendelse af passageroplysninger, især aftalen mellem EU og USA fra juli 2007. Disse ordninger er af stor interesse for den tilsynsførende, som allerede havde lejlighed til at fremsætte en række indledende bemærkninger angående Kommissionens spørgeskema om det påtænkte EU-PNR-system, som blev udsendt til relevante interessenter i december 2006 ⁽³⁾. Den tilsynsførende udtrykker tilfredshed med Kommissionens anmodning om udtalelse. Den tilsynsførende er af den opfattelse, at nærværende udtalelse bør nævnes i præamblen til Rådets afgørelse.

Forslagets kontekst

3. Formålet med forslaget er at harmonisere medlemsstaternes bestemmelser vedrørende de forpligtelser, der påhviler luftfartsselskaber, der flyver til eller fra mindst én medlemsstats område, for så vidt angår videregivelse af PNR-oplysninger til de kompetente myndigheder med henblik på at forebygge og bekæmpe terrorhandlinger og organiseret kriminalitet.
4. EU har indgået ordninger for videregivelse af PNR-oplysninger til lignende formål med USA og Canada. En første aftale, indgået med USA i maj 2004, blev afløst af en ny

⁽¹⁾ EFT L 281 af 23.11.1995, s. 31.

⁽²⁾ EFT L 8 af 12.1.2001, s. 1.

⁽³⁾ Bl.a. medlemsstaterne, databeskyttelsesmyndighederne og sammenslutninger af luftfartsselskaber. Spørgeskemaet tog sigte på forberedelse af Kommissionens konsekvensanalyse vedrørende forslaget.

aftale i juli 2007 ⁽¹⁾. En tilsvarende aftale blev indgået med Canada i juli 2005 ⁽²⁾. Herudover skal der efter planen indledes forhandlinger mellem EU og Australien om en aftale om udveksling af PNR-oplysninger, og Sydkorea forlanger også PNR-oplysninger for flyvninger til Sydkorea, uden at der dog er planer om forhandlinger på europæisk niveau på nuværende tidspunkt.

5. For EU's vedkommende skal forslaget ses som et supplement til Rådets direktiv 2004/82/EF ⁽³⁾ om transportvirksomheders forpligtelse til at fremsende oplysninger om passagerer, de såkaldte API-oplysninger, med henblik på bekæmpelse af ulovlig indvandring og forbedring af grænsekontrollen. Dette direktiv burde have været gennemført i medlemsstaternes nationale lovgivning senest den 5. september 2006. Det er imidlertid ikke alle medlemsstaterne, der har sørget for at gennemføre direktivet.

6. I modsætning til API-oplysninger (forhåndsinformation), der angiveligt skal hjælpe med til at identificere enkeltpersoner, vil PNR-oplysninger som nævnt i forslaget skulle bidrage til at foretage risikovurderinger af personer, indhente efterretningsoplysninger og finde forbindelser mellem kendte og ukendte personer.

7. Forslaget består af følgende hovedelementer:

— Luftfartsselskaberne skal stille PNR-oplysninger til rådighed for medlemsstaternes kompetente myndigheder med henblik på forebyggelse og bekæmpelse af terrorhandlinger og organiseret kriminalitet.

— Der skal i princippet udpeges en passageroplysningsenhed i hver medlemsstat, der bliver ansvarlig for at indsamle PNR-oplysninger fra luftfartsselskaberne (eller fra de udpegede dataformidlere) og for at foretage en risikovurdering af passagererne.

— De således vurderede oplysninger vil blive videregivet til de kompetente myndigheder i hver medlemsstat. Disse oplysninger vil blive udvekslet med andre medlemsstater fra sag til sag, men kun til ovennævnte formål.

— Videregivelse til lande uden for EU er underlagt yderligere betingelser.

⁽¹⁾ Aftale mellem Den Europæiske Union og Amerikas Forenede Stater om luftfartsselskabers behandling og overførsel af passagerliste (PNR)-oplysninger til United States Department of Homeland Security (DHS) (PNR-aftale 2007) (EUT L 204 af 4.8.2007, s. 18).

⁽²⁾ Aftale mellem Det Europæiske Fællesskab og Canadas regering om behandling af forhåndsinformation om passagerer og passagerlisteoplysninger (EUT L 82 af 21.3.2006, s. 15).

⁽³⁾ Rådets direktiv 2004/82/EF af 29. april 2004 om transportvirksomheders forpligtelse til at fremsende oplysninger om passagerer (EUT L 261 af 6.8.2004, s. 24).

— Oplysninger vil blive opbevaret i tretten år, heraf otte år i en inaktiv database.

— Behandlingen af oplysningerne er omfattet af (udkastet til) Rådets rammeafgørelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager (i det følgende benævnt »rammeafgørelsen om databeskyttelse«) ⁽⁴⁾.

— Et udvalg bestående af medlemsstaternes repræsentanter skal bistå Kommissionen med hensyn til protokol- og krypteringsspørgsmål samt kriterier og praksis for risikovurdering.

— Der vil blive foretaget en fornyet vurdering af afgørelsen inden tre år efter dens ikrafttrædelse.

Udtalelsens fokus

8. Det forslag, som den tilsynsførende er blevet anmodet om at udtale sig om, repræsenterer endnu et skridt i retning af rutinemæssig indsamling af oplysninger om enkeltpersoner, som i princippet ikke mistænkes for nogen forbrydelse. Som nævnt ovenfor foregår denne udvikling både på internationalt og europæisk plan.

9. Den tilsynsførende noterer sig også, at Artikel 29-Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger og Gruppen vedrørende Politi og Retsvæsen har forelagt en fælles udtalelse om forslaget ⁽⁵⁾. Den tilsynsførende støtter denne udtalelse. Nærværende udtalelse fremhæver og kommer nærmere ind på yderligere punkter.

10. Selv om alle relevante aspekter af forslaget vil blive analyseret, vil den tilsynsførende i sin udtalelse koncentrere sig om fire centrale spørgsmål.

— Det første af disse spørgsmål vedrører de påtænkte foranstaltningers legitimitet. Forslaget vil blive vurderet i henseende til formål, nødvendighed og proportionalitet på baggrund af kriterierne i artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder.

— Udtalelsen vil også analysere spørgsmålet om, hvilken lov der gælder for den foreslåede databehandling. Der vil især blive lagt vægt på anvendelsesområdet for rammeafgørelsen om databeskyttelse for så vidt angår anvendelsen af søjle 1-databeskyttelseslovgivning. Der vil også blive set nærmere på konsekvenserne af den gældende databeskyttelsesordning for udøvelsen af den registreredes rettigheder.

⁽⁴⁾ Det seneste udkast til dette forslag findes i dok. 16397/07.

⁽⁵⁾ Fælles udtalelse om forslaget til Rådets rammeafgørelse om anvendelse af passagerlister (PNR-oplysninger) med henblik på retshåndhævelse, forelagt af Kommissionen den 6. november 2007, vedtaget af Artikel 29-Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger den 5. december 2007 og af Gruppen vedrørende Politi og Retsvæsen den 18. december 2007, WP 145, WPPJ 01/07.

— Udtalelsen vil herefter fokusere på beskaffenheden af modtagerne af oplysninger på nationalt plan. Det er især beskaffenheden af passageroplysningsenhederne, dataformidlerne og de kompetente myndigheder, der er udpeget til at foretage risikovurderinger og analysere passageroplysninger, som giver anledning til betænkeligheder, da forslaget ikke indeholder nogen præciseringer i den retning.

— Det fjerde spørgsmål vedrører betingelserne for videregivelse af oplysninger til tredjelande. Det er ikke klart, hvilke betingelser der vil komme til at gælde for sådan videregivelse, når der gælder forskellige regelsæt: betingelserne for videregivelse i henhold til det foreliggende forslag, betingelserne i rammeafgåelsen om databeskyttelse og betingelserne i de eksisterende internationale aftaler (med USA og Canada).

11. Den sidste del af udtalelsen kommer ind på en række andre substansspørgsmål, bl.a. positive skridt for så vidt angår databeskyttelse, men også yderligere kilder til bekymring i forslaget.

II. DE FORESLÅEDE FORANSTALTNINGERS LEGITIMITET

12. For at analysere de foreslåede foranstaltningers legitimitet i overensstemmelse med de grundlæggende databeskyttelsesprincipper, især artikel 8 i EU-charteret om grundlæggende rettigheder og artikel 5-8 i Europarådets konvention nr. 108 ⁽¹⁾, er det nødvendigt klart at fastslå formålet med den påtænkte behandling af personoplysninger for at kunne vurdere, om kravene om nødvendighed og proportionalitet er opfyldt. Det bør sikres, at det påtænkte formål ikke kan opfyldes med andre og mindre radikale midler.

Identifikation af formålet

13. Affattelsen af forslaget og den tilhørende konsekvensanalyse tyder på, at målet ikke blot er at identificere kendte terrorister eller kendte kriminelle, der er involveret i organiseret kriminalitet, ved at sammenligne deres navne med navnene på de lister, som de retshåndhavende myndigheder forvalter. Formålet er at indsamle efterretningsoplysninger om terrorisme eller organiseret kriminalitet og mere præcist »at foretage risikovurderinger af personer, indhente efterretningsoplysninger og finde forbindelser mellem kendte og ukendte personer« ⁽²⁾. På linje hermed er formålet som fastsat i forslagets artikel 3, stk. 5, først og fremmest »at identificere personer, der er eller kan være involveret i terrorhandlinger eller organiseret kriminalitet, samt deres sammensvorne«.
14. Det er det, der bruges som begrundelse for, at API-oplysningerne ikke er tilstrækkelige til at opfylde det angivne formål. Som allerede nævnt forholder det sig nemlig således, at mens det er meningen, at API-oplysninger

skal hjælpe med til at identificere enkeltpersoner, har PNR-oplysninger ikke noget identifikationsformål, men bidrager til at foretage risikovurderinger af personer, indhente efterretningsoplysninger og finde forbindelser mellem kendte og ukendte personer.

15. Formålet med de påtænkte foranstaltninger omfatter ikke kun pågribelse af *kendte* personer, men også lokalisering af personer, der *kan* falde ind under kriterierne i forslaget.

Med henblik på at identificere disse personer er kernen i hele projektet risikovurdering og identifikation af mønstre. Det hedder udtrykkeligt i forslagets betragtning 9, at oplysninger skal »gemmes tilstrækkeligt længe til, at de kan anvendes til at udvikle risikoindikatorer og fastslå rejse- og adfærdsmønstre«.

16. Formålet beskrives således i to lag: det første lag består af det overordnede mål, nemlig at bekæmpe terrorisme og organiseret kriminalitet, mens det andet lag også omfatter de midler og foranstaltninger, der er nødvendige for at nå dette mål. Mens formålet bekæmpelse af terrorisme og organiseret kriminalitet synes klart nok og legitimt, kan midlerne til at opfylde dette formål derimod diskuteres.

Identifikation af mønstre og risikovurdering

17. Forslaget siger ikke noget om, hvordan der skal fastslås mønstre og foretages risikovurderinger. Konsekvensanalysen giver følgende præcisering af, hvordan PNR-oplysningerne vil blive anvendt: passageroplysningerne vil blive kørt »sammen med en kombination af oplysninger om karakteristika og adfærdsmønstre, der sigter mod at foretage en risikovurdering. Når en passager passer ind i en bestemt risikovurdering, kan han identificeres som en passager, der udgør en høj risiko« ⁽³⁾.
18. Mistænkte personer vil kunne udvælges på grundlag af konkrete mistænkelige elementer i deres PNR-oplysninger (f.eks. kontakt til et mistænkeligt rejsebureau eller reference til et stjålet kreditkort) såvel som på grundlag af »mønstre« eller en abstrakt profil. Der vil således kunne oprettes forskellige standardprofiler på grundlag af rejsemønstre for »normale passagerer« eller »mistænkelige passagerer«. Disse profiler åbner mulighed for yderligere efterforskning af de passagerer, der ikke falder ind under kategorien »normale passagerer«, især hvis deres profil har forbindelse til andre mistænkelige elementer som f.eks. et stjålet kreditkort.
19. Selv om man ikke kan gå ud fra, at passagerer gøres til mål for en efterforskning på grundlag af deres religion eller andre følsomme oplysninger, fremgår det ikke desto mindre, at de vil blive gjort til genstand for efterforskning på grundlag af en blanding af *konkrete* og *abstrakte* oplysninger, bl.a. standardmønstre og abstrakte profiler.

⁽¹⁾ Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger.

⁽²⁾ Forslagets begrundelse, kapitel I.

⁽³⁾ Konsekvensanalysen, kapitel 2.1 (beskrivelse af problemet).

20. Det kan diskuteres, om denne type efterforskning kan betragtes som profilering. Profilering består af en computermetode, der gør brug af data mining i et data warehouse, hvorved det bliver muligt, eller er hensigten at det skal blive muligt, med en vis sandsynlighed — og dermed også med en vis fejlmargen — at placere en enkeltperson i en bestemt kategori med det formål at træffe individuelle afgørelser med hensyn til denne person ⁽¹⁾.
21. Den tilsynsførende er klar over, at der er en debat i gang om definitionen af profilering. Men uanset om det er officielt anerkendt eller ej, at forslaget tager sigte på *profilering* af passagerer, drejer sagens kerne sig ikke om definitioner. Den drejer sig om følgerne for enkeltpersoner.
22. Den tilsynsførende er især betænkelig ved, at afgørelser om enkeltpersoner vil blive truffet på grundlag af mønstre og kriterier, der er udarbejdet på grundlag af generelle passageroplysninger. Afgørelser om en enkeltperson vil derfor muligvis blive truffet med henvisning (i det mindste til dels) til mønstre, der er udledt af *andre* personers oplysninger. Afgørelser, der kan få stor betydning for de registrerede, vil således blive truffet i relation til en abstrakt kontekst. Det er yderst vanskeligt for enkeltpersoner at forsvare sig selv mod sådanne afgørelser.
23. Hertil kommer, at der vil blive foretaget risikovurdering, uden at der findes ensartede standarder for identifikation af mistænkte. Den tilsynsførende sætter kraftigt spørgsmålstegn ved retssikkerheden i forbindelse med hele filtreringsprocessen, da de kriterier, som hver enkelt passager vil blive scannet i forhold til, er så dårligt defineret.
24. Den tilsynsførende minder om Den Europæiske Menneskerettighedsdomstols retspraksis, hvorefter national lovgivning skal være tilstrækkelig præcis til, at borgerne kan få klar besked om, under hvilke omstændigheder og på hvilke betingelser de offentlige myndigheder har kompetence til at registrere oplysninger om deres privatliv og gøre brug af disse oplysninger. Oplysningerne bør være tilgængelige for de registrerede og virkningerne heraf bør

være forudsigelige. En regel betragtes som forudsigelig, hvis den er formuleret tilstrækkelig præcist til, at enhver person — om nødvendigt med passende rådgivning — kan regulere sin adfærd ⁽²⁾.

25. Det kan konkluderes, at det især er på grund af disse typer risici, at forslaget skal overvejes nøje. Mens det generelle formål, dvs. at bekæmpe terrorisme og organiseret kriminalitet, i sig selv er klart og legitimt, synes kernen i den databehandling, der skal indføres, ikke at være tilstrækkeligt afgrænset og berettiget. Den tilsynsførende opfordrer derfor indtrængende EU-lovgiveren til at afklare dette spørgsmål, før rammeafgørelsen vedtages.

Nødvendighed

26. Som det fremgår af ovenstående, er det indlysende, at der er tale om foranstaltninger der griber ind i privatlivets fred. Men på den anden side er det langt fra bevist, at de er nyttige.
27. Forslagets konsekvensanalyse koncentrerer sig om, hvordan der bedst kan etableres en EU-PNR-ordning, snarere end om, hvorvidt en sådan ordning er nødvendig. Der henvises i konsekvensanalysen ⁽³⁾ til de PNR-systemer, der findes i andre lande, nemlig USA og Det Forenede Kongerige. Man må imidlertid beklage manglen på præcise oplysninger og tal i forbindelse med disse systemer. Der rapporteres om »mange« anholdelser for »forskellige« lovovertrædelser i det britiske semaforssystem, uden at der præciseres nogen sammenhæng med terrorisme eller organiseret kriminalitet. Der gives ikke nærmere oplysninger om det amerikanske program, bortset fra at det nævnes, at EU har haft mulighed for at vurdere værdien af PNR-oplysninger og for at erkende deres potentiale til retshåndhævelsesformål.
28. Der er ikke kun i forslaget, at der er mangel på præcise oplysninger om de konkrete resultater af sådanne PNR-systemer; rapporter, der er offentliggjort af *andre organer*, f.eks. GAO i USA, kan ikke på nuværende tidspunkt bekræfte, at foranstaltningerne er effektive ⁽⁴⁾.

⁽¹⁾ Denne definition stammer fra en undersøgelse, som Europarådet for nylig foretog af profilering: *L'application de la Convention 108 au mécanisme de profilage, Eléments de réflexion destinés au travail futur du Comité consultatif (T-PD)*, Jean-Marc Dinant, Christophe Lazaro, Yves Pouillet, Nathalie Lefever og Antoinette Rouvroy, november 2007 (endnu ikke offentliggjort). Lee Bygrave har defineret profilering i bred forstand som processen med at udlede et sæt karakteristika (typisk adfærdskarakteristika) om en enkeltperson eller en gruppe af personer og derefter behandle denne person/gruppe (eller andre personer/grupper) i lyset af disse karakteristika. Profileringsprocessen består som sådan af to hovedkomponenter: i) selve udarbejdelsen af profilen, dvs. processen med at udlede en profil, og ii) anvendelsen af profilen, dvs. processen med at behandle personer/grupper i lyset af denne profil. L.A. BYGRAVE, Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling, *Computer Law & Security Report*, 2001, Vol. 17, s. 17-24, <http://www.austlii.edu.au/journals/PLPR/2000/40.html>

⁽²⁾ Rotaru mod Rumænien, nr. 28341/95, § 50, 52 og 55. Jf. også Amann mod Schweiz, nr. 27798/95, § 50 ff.

⁽³⁾ Kapitel 2.1 (beskrivelse af problemet).

⁽⁴⁾ Se f.eks. United States Government Accountability Office — Report to Congressional Requesters »Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain«, maj 2007, <http://www.gao.gov/new.items/d07346.pdf>

29. Teknikker, der ved brug af data mining-redskaber og adfærdsmønstre går ud på at vurdere den risiko, som enkeltpersoner udgør, skal efter den tilsynsførendes opfattelse undersøges nærmere, og deres nytte i relation til bekæmpelse af terrorisme skal påvises klart, før de anvendes i så stort omfang.

Proportionalitet

30. For at vurdere balancen mellem foranstaltningens indgreb i privatlivets fred og dens nødvendighed⁽¹⁾ tages der hensyn til følgende elementer:

- Foranstaltningerne gælder for alle passagerer, uanset om de er genstand for de retshåndhævende myndigheders efterforskning eller ej. Der er tale om proaktiv forskning i en hidtil ukendt målestok.
- Afgørelser om enkeltpersoner kan baseres på abstrakte profiler, hvilket indebærer en betydelig fejlmargen.
- De foranstaltninger, der skal træffes over for den enkelte, har karakter af retshåndhævelsesforanstaltninger: konsekvenserne for så vidt angår opholdsforbud og tvangsforanstaltninger repræsenterer således et meget større indgreb end konsekvenserne i andre sammenhænge som f.eks. kreditkortbedrageri eller marketing.

31. Overholdelsen af proportionalitetsprincippet betyder ikke blot, at den foreslåede foranstaltning skal være effektiv, men også at det formål, der påtænkes med forslaget, ikke kan opfyldes med andre instrumenter, der ikke i samme grad griber ind i privatlivets fred. Der er ikke ført bevis for, at de påtænkte foranstaltninger er effektive. Det skal nøje undersøges, om der findes alternativer, før der indføres nye eller yderligere foranstaltninger til behandling af personoplysninger. Den tilsynsførende mener ikke, at der er foretaget en sådan omfattende undersøgelse.

32. Den tilsynsførende vil gerne minde om andre storstilede systemer til overvågning af enkeltpersoners bevægelser i EU eller ved EU's grænser, som enten allerede er operationelle eller er på vej til at blive det, bl.a. visuminformationssystemet⁽²⁾ og Schengeninformationssystemet⁽³⁾. Disse instrumenter har ganske vist ikke bekæmpelse af terrorisme eller organiseret kriminalitet som deres hovedmål,

men til en vis grad er de eller vil de blive tilgængelige for de retshåndhævende myndigheder med henblik på bekæmpelse af kriminalitet i bred forstand⁽⁴⁾.

33. Et andet eksempel vedrører tilgængeligheden af personoplysninger i de nationale politidatabaser, især biometriske oplysninger, inden for rammerne af Prüm-aftalen, der blev undertegnet i maj 2005 og er ved at blive udvidet til alle EU-medlemsstaterne⁽⁵⁾.

34. Disse forskellige instrumenter har alle det til fælles, at de muliggør global overvågning af enkeltpersoners bevægelser, også selv om det sker fra forskellige perspektiver. Der bør foretages en indgående og omfattende analyse af, hvordan de allerede kan bidrage til bekæmpelse af bestemte former for kriminalitet, herunder terrorisme, før det besluttet at indføre en ny form for systematisk scanning af alle personer, der ankommer til eller forlader EU med fly. Den tilsynsførende anbefaler, at Kommissionen foretager en sådan analyse som et nødvendigt skridt i lovgivningsprocessen.

Konklusion

35. På baggrund af ovenstående konkluderer den tilsynsførende følgende med hensyn til de foreslåede foranstaltningers legitimitet. Handling på grundlag af forskellige databaser, uden at der er noget samlet overblik over de konkrete resultater og mangler:

- er i modstrid med en rationel lovgivningspolitik, hvorefter der ikke må vedtages nye instrumenter, før de eksisterende instrumenter er fuldt gennemført og har vist sig at være utilstrækkelige⁽⁶⁾
- kan betyde et skridt i retning af et totalt overvågnings-samfund.

36. Bekæmpelse af terrorisme kan helt sikkert være en legitim grund til at fravige den grundlæggende ret til privatlivets fred og databeskyttelse. Men det er kun legitimt at tilside-sætte disse rettigheder, hvis det påvises klart og ubestrideligt, at dette er nødvendigt, og det skal også påvises, at

(1) Det hedder i artikel 9 i konvention nr. 108, at »artikel 5, 6 og 8 kan fraviges, når den kontraherende parts gældende lovgivning hjemler det og undtagelsen er en nødvendig forholdsregel i et demokratisk samfund for at:

1) beskytte statens sikkerhed, offentlighedens sikkerhed, statens økonomiske interesser eller for at bekæmpe strafbare forhold
2) beskytte den registrerede eller andres frihedsrettigheder og andre rettigheder».

(2) Rådets beslutning 2004/512/EF af 8. juni 2004 om indførelse af visuminformationssystemet (VIS) (EUT L 213 af 15.6.2004, s. 5). Forslag til Europa-Parlamentets og Rådets forordning om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold, KOM(2004) 835 endelig. Forslag til Rådets afgørelse om adgang til søgning i visuminformationssystemet (VIS) for de myndigheder i medlemsstaterne, der har ansvaret for den indre sikkerhed, og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger, KOM(2005) 600 endelig.

(3) Jf. især Rådets afgørelse 2007/533/RIA af 12. juni 2007 om oprettelse, drift og brug af anden generation af Schengeninformationssystemet (SIS II) (EUT L 205 af 7.8.2007).

(4) Jf. i den forbindelse udtalelsen fra Den Europæiske Tilsynsførende for Databeskyttelse om forslaget til Rådets afgørelse om adgang til søgning i visuminformationssystemet (VIS) for de myndigheder i medlemsstaterne, der har ansvaret for den indre sikkerhed, og for Europol med henblik på forebyggelse, afsløring og efterforskning af terrorhandlinger og andre alvorlige strafbare handlinger (KOM(2005) 600 endelig) (EUT C 97 af 25.4.2006, s. 6).

(5) Jf. den tilsynsførendes udtalelser om Prüm-afgørelserne: udtalelsen af 4. april 2007 om 15 medlemsstaters initiativ med henblik på vedtagelse af Rådets afgørelse om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet (EUT C 169 af 21.7.2007, s. 2), og udtalelsen af 19. december 2007 om Forbundsrepublikken Tysklands initiativ med henblik på vedtagelse af Rådets afgørelse om gennemførelse af afgørelse 2007/.../RIA om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet; disse udtalelser findes på: <http://www.edps.europa.eu>

(6) Den tilsynsførende har gjort opmærksom på dette flere gange, senest i sin udtalelse af 25. juli 2007 om gennemførelsen af databeskyttelsesdirektivet (EUT C 255 af 27.10.2007, s. 1).

databehandlingen er i overensstemmelse med proportionalitetsprincippet. Dette er så meget desto mere påkrævet i tilfælde af et så omfattende indgreb i privatlivets fred som det, der er tale om i forslaget.

37. Det kan kun bemærkes, at der ikke føres bevis herfor i forslaget, og at kravet om en nødvendigheds- og proportionalitetstest ikke er opfyldt.
38. Den tilsynsførende insisterer på, at det er væsentligt at foretage en nødvendigheds- og proportionalitetstest som nævnt ovenfor. Dette er en absolut betingelse for forslagets ikrafttræden. Alle videre bemærkninger fra den tilsynsførende i nærværende udtalelse skal ses i lyset af denne indledende betingelse.

III. GÆLDENDE LOV — UDØVELSE AF DEN REGISTREREDES RETTIGHEDER

Gældende lov

39. Analysen nedenfor er koncentreret om tre punkter:
- en beskrivelse af de forskellige skridt i den databehandling, der er forudsat i forslaget, med henblik på at fastslå, hvilken lov der gælder på hvert trin
 - begrænsningerne i rammeafgørelsen om databeskyttelse for så vidt angår anvendelsesområde og den registreredes rettigheder
 - en mere generel analyse af, i hvilket omfang et søjle 3-instrument kan gælde for private aktører, der foretager databehandling i søjle 1-kontekst.

Gældende lov på de forskellige trin af databehandlingen

40. I forslagets artikel 11 hedder det, at »medlemsstaterne sikrer, at Rådets rammeafgørelse (...) om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejde finder anvendelse på behandlingen af oplysninger i medfør af denne rammeafgørelse«.
41. Til trods for denne bestemmelse er det imidlertid ikke klart, i hvilket omfang rammeafgørelsen om databeskyttelse — et instrument i henhold til EU-traktatens søjle 3 — gælder for oplysninger, der behandles af luftfartsselskaber, indsamles af passageroplysningsenheder og videregives af andre kompetente myndigheder.
42. Det første skridt i behandlingen af personoplysninger er ifølge forslaget luftfartsselskabernes behandling; luftfartsselskaberne er forpligtet til at stille PNR-oplysninger til

rådighed for de nationale passageroplysningsenheder, i princippet ved brug af pushmetoden. Det synes at fremgå af teksten til forslaget og konsekvensanalysen ⁽¹⁾, at luftfartsselskaberne også kan videregive oplysninger til dataformidlerne som bulkdata. Luftfartsselskaberne er fortrinsvis aktive i et kommercielt miljø og er underlagt den nationale databeskyttelseslovgivning, der gennemfører direktiv 95/46/EF ⁽²⁾. Der vil opstå spørgsmål vedrørende gældende lov, når de indsamlede oplysninger anvendes til retshåndhævelsesformål ⁽³⁾.

43. Oplysningerne vil herefter blive filtreret af en dataformidler (de vil blive formateret, og de PNR-oplysninger, der ikke er med på listen over oplysninger som krævet i forslaget, vil blive frasortet) eller tilsendt passageroplysningsenhederne direkte. Dataformidlere kan også være aktører fra den private sektor, som det er tilfældet med SITA, der opererer i den forstand inden for rammerne af PNR-aftalen med Canada.

44. Når det drejer sig om passageroplysningsenhederne, der har ansvaret for risikovurderingen af den samlede mængde oplysninger, er det ikke klart, hvem der bliver ansvarlig for behandlingen. Told- og grænsemyndighederne kan blive involveret og ikke nødvendigvis de retshåndhævende myndigheder.

45. Den efterfølgende videregivelse af filtrerede oplysninger til de »kompetente« myndigheder vil sandsynligvis foregå i en retshåndhævelseskontekst. Det hedder i forslaget: »De kompetente myndigheder omfatter kun de myndigheder, der er ansvarlige for forebyggelse eller bekæmpelse af terrorhandlinger og organiseret kriminalitet«.

46. Jo længere behandlingen af oplysningerne skrider frem, jo tættere forbindelse bliver der mellem på den ene side de involverede aktører og det tilstræbte formål og på den anden side politisamarbejdet og det retlige samarbejde i straffesager. Forslaget nævner imidlertid ikke udtrykkeligt, præcist hvornår rammeafgørelsen om databeskyttelse finder anvendelse. Affattelsen kunne endog tyde på, at den finder anvendelse på hele behandlingen, selv på luftfartsselskaberne ⁽⁴⁾. Rammeafgørelsen om databeskyttelse indeholder dog i sig selv nogle begrænsninger.

⁽¹⁾ Forslaget, artikel 6, stk. 3, og konsekvensanalysen, bilag A (metoden til luftfartsselskabernes videregivelse af oplysninger).

⁽²⁾ Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281 af 23.11.1995, s. 31).

⁽³⁾ Jf. i den forbindelse følgerne af PNR-dommen. Domstolens dom af 30. maj 2006, Europa-Parlamentet mod Rådet (C-317/04) og Kommissionen (C-318/04), de forenede sager C-317/04 og C-318/04, Sml. 2006, præmis 56.

⁽⁴⁾ Artikel 11 i forslaget. Se også betragtning 10 i præamblen: »Rådet rammeafgørelse (...) om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejde bør finde anvendelse på alle oplysninger, der behandles i overensstemmelse med denne rammeafgørelse. De registreredes rettigheder i forbindelse med denne behandling, såsom retten til at blive informeret, at få adgang til oplysningerne, at korrigere, slette eller blokere dem samt til at klage og få kompensation, bør fastsættes inden for rammerne af denne rammeafgørelse«.

47. I denne kontekst sætter den tilsynsførende grundlæggende spørgsmålstegn ved, om EU-traktatens afsnit VI kan bruges som retsgrundlag for, at aktører i den private sektor rutinemæssigt pålægges retlige forpligtelser til retshåndhævelsesformål. Derudover er det også relevant, om EU-traktatens afsnit VI kan bruges som retsgrundlag for, at offentlige myndigheder, der i princippet befinder sig uden for rammerne af retshåndhævelsessamarbejdet, pålægges retlige forpligtelser. Udtalelsen vil komme nærmere ind på disse spørgsmål.

Begrænsninger i rammeafgårelsen om databeskyttelse

48. Teksten til rammeafgårelsen om databeskyttelse indeholder mindst to begrænsninger, som er relevante for dens anvendelsesområde.

49. For det første er anvendelsesområdet for rammeafgårelsen om databeskyttelse udmærket defineret i selve rammeafgårelsen: den »finder kun anvendelse på oplysninger, der er indsamlet eller behandlet af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner«⁽¹⁾.

50. For det andet er det ikke meningen, at rammeafgårelsen om databeskyttelse skal finde anvendelse på oplysninger, der udelukkende behandles på nationalt plan, idet den er begrænset til oplysninger, der udveksles mellem medlemsstaterne, og videregivelsen heraf til tredjelande⁽²⁾.

51. Der er også nogle punkter, hvor rammeafgårelsen om databeskyttelse er et tilbageskridt i forhold til direktiv 95/46/EF, især den brede undtagelse fra princippet om formålsbegrænsning. Hvad angår formålsprincippet begrænser forslaget klart formålet med behandlingen til bekæmpelse af terrorisme og organiseret kriminalitet. Rammeafgårelsen om databeskyttelse tillader derimod behandling til bredere formål. I et sådant tilfælde bør *lex specialis* (forslaget) have forrang for *lex generalis* (rammeafgårelsen om databeskyttelse)⁽³⁾. Dette bør nævnes udtrykkeligt i teksten til forslaget.

52. Af den grund anbefaler den tilsynsførende at tilføje følgende bestemmelse i forslaget: »Personoplysninger, der videregives af luftfartsselskaber i henhold til denne rammeafgårelse, må ikke behandles til andre formål end bekæmpelse af terrorisme og organiseret kriminalitet. Undtagelserne fra formålsprincippet i Rådets rammeafgårelse om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager finder ikke anvendelse«.

(1) Betragtning 5a i rammeafgårelsen om databeskyttelse, udgaven af 11. december 2007.

(2) Artikel 1.

(3) Hvad angår dette punkt bør teksten til artikel 27b i det seneste udkast til rammeafgårelsen om databeskyttelse i søjle 3 nøje overvejes og drøftes.

53. Den tilsynsførende konkluderer, at der er alvorlig mangel på retssikkerhed med hensyn til, hvilken databeskyttelsesordning der gælder for de forskellige aktører, der er involveret i projektet, og især for luftfartsselskaber og andre søjle 1-aktører, dvs. om det er reglerne i forslaget, reglerne i rammeafgårelsen om databeskyttelse eller den nationale lovgivning til gennemførelse af direktiv 95/46/EF. Lovgiveren bør gøre det klart, præcist på hvilket trin af behandlingen disse forskellige regler finder anvendelse.

Betingelserne for anvendelse af søjle 1- og søjle 3-reglerne

54. Den tilsynsførende sætter grundlæggende spørgsmålstegn ved den omstændighed, at et søjle 3-instrument rutinemæssigt og til retshåndhævelsesformål skaber retlige forpligtelser for aktører i den private eller offentlige sektor, der i princippet befinder sig uden for rammerne af retshåndhævelsessamarbejdet.

55. Der kan her sammenlignes med to andre sager, hvor den private sektor var involveret i opbevaring eller videregivelse af oplysninger med henblik på retshåndhævelse:

— *Den amerikanske PNR-sag, hvor der var planer om luftfartsselskabernes systematiske videregivelse af PNR-oplysninger til de retshåndhævende myndigheder.* Domstolens dom i PNR-sagen udelukkede, at Fællesskabet havde kompetence til at indgå PNR-aftalen. En af begrundelserne var, at videregivelsen af PNR-oplysninger til det amerikanske CBP (Bureau of Customs and Border Protection) udgør behandling, der vedrører den offentlige sikkerhed og statens aktiviteter på det strafferetlige område⁽⁴⁾. I denne sag bestod behandlingen i systematisk videregivelse til CBP, hvilket adskiller den fra den følgende sag:

— *Elektroniske kommunikationsudbydere almindelige opbevaring af data.* Hvad angår Fællesskabets kompetence til at fastsætte en sådan opbevaringsperiode, adskiller denne sag sig fra den amerikanske PNR-sag, da der i henhold til direktiv 2006/24/EF⁽⁵⁾ kun gælder en opbevaringsforpligtelse, når dataene forbliver under udbydernes kontrol. Der er ikke tale om nogen automatisk videregivelse af data til de retshåndhævende myndigheder. Det kan konkluderes, at så længe dataene forbliver under tjenesteudbydernes kontrol, er disse udbydere også ansvarlige for opfyldelsen af forpligtelserne angående beskyttelse af de registreredes personoplysninger.

(4) Domstolens dom af 30. maj 2006, Europa-Parlamentet mod Rådet (C-317/04) og Kommissionen (C-318/04), i de forenede sager C-317/04 og C-318/04, Sml. 2006, præmis 56.

(5) Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT L 105 af 13.4.2006, s. 54).

56. I det foreliggende EU-PNR-forslag skal luftfartsselskaberne systematisk stille PNR-oplysninger om alle passagerer til rådighed. Disse oplysninger videregives imidlertid ikke direkte til de retshåndhævende myndigheder som bulkdata: de kan sendes til en dataformidler, og de vurderes af en tredjepart, hvis status fortsat er uklar, før udvalgte oplysninger videregives til de kompetente myndigheder.
57. Hovedparten af behandlingen foregår i en gråzone med materielle forbindelser til både søjle 1 og 3. Som vi kommer nærmere ind på i kapitel IV, er databehandlingsaktørernes beskaffenhed ikke klar. Luftfartsselskaber er selvsagt ikke retshåndhævende myndigheder, og dataformidlere kan være aktører i den private sektor. Selv i forbindelse med passageroplysningsenhederne, der vil være offentlige myndigheder, skal det understreges, at det ikke er alle offentlige myndigheder, der er af en sådan beskaffenhed og har en sådan kompetence, at de rutinemæssigt kan udføre retshåndhævelsesopgaver.
58. Der har traditionelt været en klar adskillelse mellem retshåndhævelsesaktiviteter og den private sektors aktiviteter, således at retshåndhævelsesopgaver er blevet udført af særlige myndigheder, især politiet, og den private sektor fra sag til sag er blevet anmodet om at videregive personoplysninger til disse håndhævelsesmyndigheder. Der er nu en tendens til systematisk at pålægge private aktører samarbejde med henblik på retshåndhævelse, hvilket rejser spørgsmålet om, hvilken databeskyttelsesramme (søjle 1 eller 3) der gælder for betingelserne for dette samarbejde: bør reglerne baseres på beskaffenheden af den dataansvarlige (den private sektor) eller på det tilstræbte formål (retshåndhævelse)?
59. Den tilsynsførende har allerede gjort opmærksom på risikoen for et juridisk tomrum mellem søjle 1- og søjle 3-aktiviteter⁽¹⁾. Det er således langt fra klart, om private selskabers aktiviteter, der på den ene eller den anden måde hænger sammen med håndhævelse af strafferetten, er omfattet af området for EU-lovgiverens handling i henhold til artikel 30, 31 og 34 i TEU.
60. Hvis den almindelige ramme (søjle 1) ikke finder anvendelse, vil en tjenesteudbyder være nødt til at foretage vanskelige sondringer i sine databaser. Ifølge den nuværende ordning er det klart, at den dataansvarlige skal overholde samme databeskyttelse i forhold til de registrerede, uanset hvilket formål der begrunder opbevaringen af oplysningerne. Et resultat, der betyder, at tjenesteudbydere behandler oplysninger til forskellige formål bliver omfattet af forskellige databeskyttelsesrammer, bør derfor undgås.

⁽¹⁾ Jf. udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om opfølgning på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet (EUT C 255 af 27.10.2007, s. 1). Jf. også årsrapporten 2006, s. 47.

Udøvelse af den registreredes rettigheder

61. De forskellige retlige ordninger, der vil komme til at gælde på nationalt plan, får store virkninger, navnlig for den registreredes udøvelse af sine rettigheder.
62. Det hedder i præamblen til forslaget, at retten til at blive informeret, at få adgang til oplysningerne, at korrigere, slette eller blokere dem samt til at klage og få kompensation bør fastsættes inden for rammerne af rammeafgørelsen om databeskyttelse. Dette besvarer imidlertid ikke spørgsmålet om, hvem den dataansvarlige er, der skal behandle anmodninger fra de registrerede.
63. Mens oplysninger om behandlingen kunne gives af luftfartsselskaberne, er spørgsmålet mere komplekst, når det drejer sig om adgang til eller korrektion af oplysninger. Disse rettigheder er nemlig begrænset i henhold til rammeafgørelsen om databeskyttelse. Som nævnt ovenfor er det tvivlsomt, om en tjenesteudbyder som f.eks. et luftfartsselskab kan pålægges at indrømme forskellige rettigheder med hensyn til adgang til og korrektion af de oplysninger, vedkommende er i besiddelse af, alt efter det tilstræbte formål (kommercielt formål eller retshåndhævelse). Det kunne eventuelt argumenteres, at disse rettigheder skal udøves over for passageroplysningsenheden eller de på anden måde udpegede kompetente myndigheder. Men forslaget giver ikke nærmere oplysninger i den henseende, og det er som allerede nævnt ikke klart, om disse myndigheder (i det mindste passageroplysningsenhederne) bliver de retshåndhævende myndigheder, der normalt står for procedurerne for begrænset (eventuelt indirekte) adgang.
64. Den enkelte risikerer også at blive konfronteret med forskellige modtagere af oplysninger, når der er tale om passageroplysningsenhederne: oplysningerne videregives således til passageroplysningsenheden i flyenes afgang- og ankomstland, men eventuelt også fra sag til sag til passageroplysningsenheder i andre medlemsstater. Det er desuden muligt, at flere medlemsstater opretter eller udpeger én fælles passageroplysningsenhed. Den registrerede kan i så fald være nødt til at udøve sin klageret over for en myndighed i en anden medlemsstat. Heller ikke her er det klart, om de nationale databeskyttelsesregler finder anvendelse (de formodes at være harmoniseret i EU), eller om der vil skulle tages hensyn til specifik retshåndhævelseslovgivning (i mangel af en generel harmonisering inden for søjle 3 på nationalt plan).
65. Det samme spørgsmål gør sig gældende for så vidt angår adgangen til oplysninger, der behandles af dataformidlere, hvis status er uklar, og som også kan være fælles for luftfartsselskaber fra flere EU-medlemsstater.

66. Den tilsynsførende beklager den usikkerhed, der fortsat består med hensyn til den registreredes udøvelse af disse grundlæggende rettigheder. Han understreger, at denne situation mest skyldes, at aktører, der ikke har retshåndhævelse som deres hovedopgave, pålægges et sådant ansvar.

Konklusion

67. Den tilsynsførende er af den opfattelse, at forslaget bør gøre det klart, hvilken retlig ordning der finder anvendelse på hvilket trin af databehandlingen, og desuden præcisere, over for hvilken aktør eller myndighed retten til adgang og klage skal udøves. Den tilsynsførende minder om, at i henhold til artikel 30, stk. 1, litra b), i TEU bør databeskyttelsesbestemmelserne være relevante og omfatte hele det spektrum af behandlingsoperationer, der er fastsat i forslaget. Det er ikke nok med en simpel henvisning til rammeafgårelsen om databeskyttelse i betragtning af dennes begrænsede anvendelsesområde og den rettighedsbegrænsning, den indebærer. Når de retshåndhævende myndigheder er involveret, bør reglerne i rammeafgårelsen om databeskyttelse i det mindste gælde for hele den databehandling, der er forudsat i forslaget, for at sikre konsekvent anvendelse af databeskyttelsesprincipperne.

IV. MODTAGERNES BESKAFFENHED

68. Den tilsynsførende bemærker, at forslaget ikke indeholder nogen nærmere præcisering af beskaffenheden af modtagerne af de personoplysninger, som luftfartsselskaberne indsamler, hvad enten der er tale om dataformidlere, passageroplysningsenheder eller kompetente myndigheder. Det skal understreges, at modtagerens beskaffenhed hænger direkte sammen med den type databeskyttelsesgarantier, der gælder for denne modtager. Forskellen mellem de garantier, der gives i navnlig søjle 1- og søjle 3-reglerne, er allerede blevet nævnt. Det er væsentligt, at den gældende ordning er klar for alle involverede aktører, herunder nationale regeringer, retshåndhævelsesorganer og databeskyttelsesmyndigheder, såvel som for de involverede dataansvarlige og registrerede.

Dataformidlere

69. Forslaget indeholder ingen nærmere oplysninger om dataformidlernes beskaffenhed⁽¹⁾. Dataformidlernes rolle som dataansvarlige eller registerførere præciseres heller ikke. Erfaringsmæssigt ser det ud til, at det udmærket kan overlades til en enhed i den private sektor, hvad enten det er et edb-reservationssystem eller en anden enhed, at indsamle PNR-oplysninger direkte fra luftfartsselskaberne for at

videregive dem til passageroplysningsenhederne. Det er netop sådan, oplysninger behandles i henhold til PNR-aftalen med Canada. SITA⁽²⁾ er det selskab, der er ansvarligt for at behandle oplysningerne. Dataformidlerens rolle er afgørende, da denne kan være ansvarlig for at filtrere eller omformatere de oplysninger, som luftfartsselskaberne videregiver som bulkdata⁽³⁾. Selv om dataformidlerne har pligt til at slette behandlede oplysninger, så snart de er videregivet til passageroplysningsenhederne, er selve behandlingen yderst følsom: en følge af dataformidlernes intervention er, at der skabes endnu en database, der indeholder enorme mængder oplysninger og endog ifølge forslaget følsomme oplysninger (dataformidlerne har så pligt til at slette disse følsomme oplysninger). Af disse grunde anbefaler den tilsynsførende, at dataformidlere ikke involveres i behandlingen af passageroplysninger, medmindre deres beskaffenhed og opgaver er nøje præciseret.

Passageroplysningsenheder

70. Passageroplysningsenhederne har en afgørende rolle med hensyn til at identificere personer, der er eller kan være involveret i eller have tilknytning til terrorisme eller organiseret kriminalitet. Ifølge forslaget vil de få ansvaret for at indføre risikoindikatorer og tilvejebringe efterretningsoplysninger om rejsemønstre⁽⁴⁾. Hvis risikovurderingen er baseret på standardiserede rejsemønstre og ikke på materielt bevismateriale i relation til en konkret sag, kan analysen betragtes som proaktiv efterforskning. Den tilsynsførende understreger, at denne form for behandling i princippet er underlagt strenge regler i medlemsstaternes lovgivning (hvis den da ikke er forbudt), og den er forbeholdt særlige offentlige myndigheder, hvis funktionsmåde også er underlagt strenge regler.
71. Passageroplysningsenhederne pålægges således en meget følsom behandling af oplysninger, uden at forslaget indeholder nogen nærmere præcisering af deres beskaffenhed og de betingelser, hvorunder de vil skulle udøve denne kompetence. Selv om denne opgave sandsynligvis vil blive udført af et offentligt organ, eventuelt toldmyndighederne eller grænsekontrollen, er forslaget ikke udtrykkeligt til hinder for, at medlemsstaterne kan overlade opgaven til efterretningsorganer eller en hvilken som helst registerfører. Den tilsynsførende understreger, at den gennemsigthed og de garantier, der gælder for efterretningsorganer, ikke altid er de samme som dem, der gælder for traditionelle retshåndhævende myndigheder. Det er absolut nødvendigt at præcisere passageroplysningsenhedernes beskaffenhed, eftersom denne vil få direkte konsekvenser for, hvilken retlig ramme, der er gældende, og tilsynsbetingelserne. Den tilsynsførende er af den opfattelse, at forslaget skal indeholde en supplerende bestemmelse med en nærmere præcisering af passageroplysningsenhedernes karakteristika.

⁽²⁾ SITA blev oprettet i 1949 af elleve medlemsluftfartsselskaber. Der leveres fordelagtige løsninger til luftfartssektoren gennem det erhvervsdrivende selskab SITA INC (Information, Networking Computing) og netværkstjenester gennem SITA SC på kooperativ basis.

⁽³⁾ Konsekvensanalysen, bilag A (metoden til luftfartsselskabernes videregivelse af oplysninger).

⁽⁴⁾ Artikel 3 i forslaget.

⁽¹⁾ Artikel 6 i forslaget.

Kompetente myndigheder

72. Det fremgår af artikel 4 i forslaget, at alle myndigheder, der er ansvarlige for forebyggelse eller bekæmpelse af terrorhandlinger og organiseret kriminalitet, kan modtage oplysningerne. Mens formålet er klart defineret, står der ikke noget om myndighedernes beskaffenhed. Forslaget begrænser på ingen måde modtagerne til de retshåndhævende myndigheder.

Som nævnt ovenfor i forbindelse med passageroplysningsenhederne er det afgørende, at denne type følsomme oplysninger behandles i et miljø med en klar retlig ramme. Dette er i højere grad tilfældet for f.eks. retshåndhævende myndigheder end for efterretningsorganer. I betragtning af de data mining-elementer og den proaktive forskning, der er omhandlet i forslaget, kan det ikke udelukkes, at sådanne efterretningsorganer involveres i behandlingen af oplysningerne, uden at andre typer myndigheder dermed udelukkes.

Konklusion

73. Den tilsynsførende har den generelle bemærkning, at håndhævelsen af et EU-PNR-system bliver endnu vanskeligere, fordi de retshåndhævende myndigheder alt efter medlemsstaternes nationale lovgivning har forskellige beføjelser, der i nogle medlemsstater, men ikke i andre, omfatter efterretning, skat, indvandring og politi. Dette er imidlertid blot endnu en grund til at anbefale, at forslaget gøres meget mere præcist med hensyn til de nævnte aktørers beskaffenhed og garantiene angående kontrollen med udførelsen af deres opgaver. Der bør indsættes yderligere bestemmelser i forslaget for nøje at præcisere dataformidlernes, passageroplysningsenhedernes og de andre kompetente myndigheders beføjelser og retlige forpligtelser.

V. BETINGELSER FOR VIDEREGIVELSE TIL TREDJELANDE

74. Forslaget giver visse garantier med hensyn til videregivelse af PNR-oplysninger til tredjelande⁽¹⁾. Navnlige fastsættes det udtrykkeligt, at rammeafgårelsen om databeskyttelse skal gælde for videregivelse af oplysninger, der opstilles en specifik formålsbegrænsning, og videreformidling kræver en medlemsstats samtykke. Videregivelse skal også være i overensstemmelse med den pågældende medlemsstats nationale ret og alle gældende internationale aftaler.
75. Der er imidlertid mange ubesvarede spørgsmål, især for så vidt angår samtykkets beskaffenhed, betingelserne for anvendelse af rammeafgårelsen om databeskyttelse og gensidighedsaspektet af videregivelsen af oplysninger til tredjelande.

⁽¹⁾ Artikel 8 i forslaget.

Samtykkets beskaffenhed

76. Oprindelsesmedlemsstaten skal give sit udtrykkelige samtykke til videregivelse af oplysninger fra det ene tredjeland til det andet. Forslaget præciserer ikke, under hvilke betingelser og af hvem dette samtykke skal gives, og heller ikke, om de nationale databeskyttelsesmyndigheder (DPA) bør involveres i afgørelsen. Den tilsynsførende er af den opfattelse, at samtykket i det mindste skal gives i overensstemmelse med de nationale love om betingelserne for videregivelse af personoplysninger til tredjelande.
77. Desuden bør en medlemsstats samtykke ikke veje tungere end princippet om, at modtagerlandet skal sørge for et tilstrækkeligt beskyttelsesniveau i forbindelse med den påtænkte behandling. Disse betingelser bør være kumulative, således som de er det i rammeafgårelsen om databeskyttelse (artikel 14). Den tilsynsførende foreslår derfor, at der i artikel 8, stk. 1, i forslaget tilføjes et litra c) med følgende ordlyd: »og c) det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau for den påtænkte behandling af oplysningerne«. Den tilsynsførende minder i den forbindelse om, at der skal indføres mekanismer til sikring af fælles standarder og koordinerede afgørelser med hensyn til tilstrækkelighed⁽²⁾.

Anvendelse af rammeafgårelsen om databeskyttelse

78. Forslaget henviser til de betingelser og garantier, der er indeholdt i rammeafgårelsen om databeskyttelse, men præciserer også udtrykkeligt visse andre betingelser, især ovennævnte samtykke fra den pågældende medlemsstat, og begrænser formålet til forebyggelse og bekæmpelse af terrorhandlinger og organiseret kriminalitet.
79. Rammeafgårelsen om databeskyttelse indeholder betingelser for videregivelse af personoplysninger til tredjelande, nemlig med hensyn til formålsbegrænsning, modtagerens beskaffenhed, medlemsstatssamtykke og tilstrækkelighedsprincippet. Den indeholder imidlertid også undtagelser fra disse betingelser for videregivelse: legitime vigtige interesser, navnlig vigtige offentlige interesser, kan udgøre et tilstrækkeligt grundlag for videregivelse, også selv om ovennævnte betingelser ikke er opfyldt.
80. Som allerede nævnt i kapitel III i denne udtalelse er den tilsynsførende af den opfattelse, at det skal fastsættes tydeligt i teksten til forslaget, at de mere præcise garantier i forslaget har forrang for de almindelige betingelser — og undtagelser — i rammeafgårelsen om databeskyttelse, hvor den finder anvendelse.

⁽²⁾ Den tilsynsførendes udtalelse af 26. juni 2007 om forslaget til Rådets rammeafgårelse om beskyttelse af personoplysninger i forbindelse med det politimæssige og strafferetlige samarbejde, punkt 27-30 (EUT C 139 af 23.6.2007, s. 1).

Gensidighed*Lande, der har en bilateral aftale med EU*

81. Forslaget behandler spørgsmålet om eventuel »modkrav« fra lande, der måtte anmode EU om PNR-oplysninger for flyvninger fra EU til deres lande. Når EU anmoder om oplysninger fra tredjelandsluftfartsselskabers databaser, fordi de foretager flyvninger til eller fra EU, vil disse tredjelande muligvis forlange det samme af luftfartsselskaber, der er etableret i EU, herunder oplysninger om EU-borgere. Selv om Kommissionen mener, at denne situation i praksis »næppe vil opstå«, gives der dog mulighed herfor. Det nævnes i den forbindelse i forslaget, at der i aftalerne med USA og Canada er fastsat bestemmelser om en sådan gensidighed, »der automatisk kan håndhæves«⁽¹⁾. Den tilsynsførende sætter spørgsmålstegn ved betydningen af en sådan automatisk gensidighed og anvendelsen af garantier i forbindelse med en sådan videregivelse af oplysninger, især eksistensen af et tilstrækkeligt beskyttelsesniveau i det pågældende land.
82. Der bør skelnes mellem tredjelande, der allerede har indgået en aftale med EU, og tredjelande, der ikke har nogen aftale.
- Lande, der ikke har nogen aftale med EU*
83. Den tilsynsførende bemærker, at gensidighed vil kunne føre til videregivelse af personoplysninger til lande, hvor der ikke kan gives garantier med hensyn til demokratiske standarder og et tilstrækkeligt databeskyttelsesniveau.
84. Konsekvensanalysen indeholder yderligere elementer hvad angår betingelserne for videregivelse af oplysninger til tredjelande: fordelene ved EU-PNR-systemet, hvor oplysningerne filtreres af passageroplysningsenheder, fremhæves. Kun udvalgte oplysninger om mistænkte enkeltpersoner (og ikke bulkdata) vil blive videregivet til medlemsstaternes kompetente myndigheder og formodentlig også til tredjelande⁽²⁾. Den tilsynsførende anbefaler at tydeliggøre dette punkt i teksten til forslaget. En simpel omtale heraf i konsekvensanalysen giver ikke den nødvendige beskyttelse.
85. Udvalget af passageroplysningerne vil ganske vist bidrage til at minimere følgerne for privatlivets fred, men der mindes om, at databeskyttelsesprincipperne rækker langt videre end dataminimering og omfatter principper som nødvendighed, gennemsigtighed og udøvelse af den registreredes rettigheder; der skal tages hensyn til alle disse principper, når der tages stilling til, om et tredjeland har et tilstrækkeligt beskyttelsesniveau.
86. Ifølge konsekvensanalysen får EU i forbindelse med sådan databehandling mulighed for at insistere på visse standarder og for at sikre konsekvensen i disse bilaterale aftaler med tredjelande. Tredjelande, som EU har en aftale med, får også mulighed for at forlange gensidig behandling, hvilket ikke er muligt i dag⁽³⁾.
87. Disse bemærkninger fører det spørgsmål med sig, hvilken virkning forslaget får for de eksisterende aftaler med Canada og USA. Betingelserne for adgang til oplysninger i disse aftaler er således meget bredere, da oplysningerne ikke er underkastet en lignende udvælgelse, før de videregives til disse tredjelande.
88. Det hedder i konsekvensanalysen, at i de tilfælde, hvor EU har en international aftale med et tredjeland om udveksling/videregivelse af PNR-oplysninger til dette tredjeland, bør der tages behørigt hensyn til en sådan aftale. Luftfartsselskaberne vil skulle sende PNR-oplysningerne til passageroplysningsenhederne i overensstemmelse med almindelig praksis i henhold til den nuværende foranstaltning. Passageroplysningsenheder, der modtager sådanne oplysninger, videregiver dem til den kompetente myndighed i det tredjeland, som der er indgået en sådan aftale med⁽⁴⁾.
89. Mens forslaget på den ene side *kun* synes at tage sigte på videregivelse af *udvalgte* oplysninger til en kompetent myndighed i EU eller i et tredjeland, gør konsekvensanalysen, præambelen til forslaget (betragtning 21) og artikel 11 i selve forslaget på den anden side opmærksom på, at der bør tages behørigt hensyn til eksisterende aftaler. Det kan måske udledes heraf, at filtrering kun vil kunne bruges i forbindelse med fremtidige aftaler. Det kan med henblik herpå forudses, at bulkadgang stadig vil være hovedreglen for f.eks. de amerikanske myndigheders adgang til PNR-oplysninger, jf. bestemmelserne i aftalen mellem EU og USA, men at der sideløbende hermed fra sag til sag kan videregives specifikke oplysninger til USA som identificeret af passageroplysningsenhederne, herunder — men ikke udelukkende — oplysninger vedrørende flyvninger til USA.
90. Den tilsynsførende beklager manglen på klarhed på dette afgørende punkt i forslaget. Han anser det for at være af allerstørste vigtighed, at betingelserne for videregivelse af PNR-oplysninger til tredjelande er konsekvente, og at der fastlægges et harmoniseret beskyttelsesniveau for videregivelsen. Af hensyn til retssikkerheden bør de garantier, der gælder for videregivelsen af oplysninger, endvidere præciseres i selve forslaget og ikke blot i konsekvensanalysen, som det er tilfældet for øjeblikket.

⁽¹⁾ Forslagets begrundelse, kapitel 2.⁽²⁾ Konsekvensanalysen, kapitel 5.2 (beskyttelse af privatlivets fred).⁽³⁾ Konsekvensanalysen, kapitel 5.2 (forbindelserne med tredjelande).⁽⁴⁾ Konsekvensanalysen, bilag A (organer, der modtager oplysninger fra passageroplysningsenhederne).

VI. ANDRE VÆSENTLIGE PUNKTER

Automatiseret behandling

91. Den tilsynsførende bemærker, at forslaget udtrykkeligt udelukker, at passageroplysningsenhederne og medlemsstaternes kompetente myndigheder træffer retshåndhævelsesforanstaltninger alene på grundlag af en automatiseret behandling af PNR-oplysninger eller på grundlag af en persons race eller etniske baggrund, religiøse eller filosofiske overbevisning, politiske holdning eller seksuelle orientering ⁽¹⁾.
92. En sådan præcisering er velkommen, da den begrænser risikoen for vilkårlige foranstaltninger over for den enkelte. Den tilsynsførende bemærker dog, at dens anvendelsesområde er begrænset til passageroplysningsenheders og kompetente myndigheders *retshåndhævelsesforanstaltninger*. Den udelukker i sin nuværende ordlyd ikke automatiseret filtrering af enkeltpersoner på grundlag af standardprofiler og hindrer heller ikke automatiseret oprettelse af lister over mistænkte personer og iværksættelse af foranstaltninger såsom udvidet overvågning, så længe disse foranstaltninger ikke betragtes som retshåndhævelsesforanstaltninger.
93. Den tilsynsførende finder, at begrebet *retshåndhævelsesforanstaltninger* er for vagt, og at der som et princip ikke bør træffes afgørelser angående enkeltpersoner alene på grundlag af en automatiseret behandling af deres oplysninger ⁽²⁾. Den tilsynsførende anbefaler at ændre teksten i den henseende.

Oplysningernes beskaffenhed

94. Artikel 5, stk. 2, i forslaget indeholder en vigtig præcisering, idet det gøres klart, at luftfartsselskaberne ikke er forpligtet til at indsamle eller opbevare oplysninger ud over dem, der indsamles til det oprindelige kommercielle formål.
95. Der er flere aspekter af behandlingen af disse oplysninger, der bør kommenteres yderligere:
- De oplysninger, der skal stilles til rådighed, jf. bilag I til forslaget, er meget omfattende, og listen svarer til listen over de oplysninger, der er til rådighed for de amerikanske myndigheder, jf. aftalen mellem EU og USA. Databeskyttelsesmyndighederne og især Artikel 29-Gruppen har allerede ved flere lejligheder sat spørgsmålstegn ved beskaffenheden af nogle af de oplysninger, der kræves ⁽³⁾.

— Det synes at fremgå af konsekvensanalysen ⁽⁴⁾ og artikel 6, stk. 3, i forslaget, at luftfartsselskaberne også kan videregive bulkdata til dataformidlerne. I første omgang vil oplysninger, der videregives til en tredjepart, ikke en gang blive begrænset i overensstemmelse med de PNR-oplysninger, der er opført på listen i bilag I til forslaget.

— Hvad angår behandlingen af følsomme oplysninger kan disse oplysninger ganske vist filtreres væk på dataformidlerstadiet, men det er stadig et spørgsmål, om det er strengt nødvendigt, at luftfartsselskaber videregiver det åbne felt.

Den tilsynsførende støtter de punkter, der blev fremsat i den henseende i Artikel 29-Gruppens udtalelse.

Metode til videregivelse af PNR-oplysninger

96. Luftfartsselskaber, der er etableret uden for EU, skal videregive oplysninger til passageroplysningsenhederne eller dataformidlerne efter *pushmetoden*, forudsat at de er i besiddelse af den nødvendige tekniske arkitektur. I modsat fald vil de være nødt til at tillade udtræk af oplysninger efter *pullmetoden*.
97. Hvis der gives mulighed for forskellige metoder til videregivelse af oplysninger, alt efter hvilket luftfartsselskab der er tale om, vil det blot gøre det vanskeligere at kontrollere, om videregivelsen af PNR-oplysninger er i overensstemmelse med databeskyttelsesreglerne. Dette risikerer også at forvride konkurrencen mellem EU- og ikke-EU-luftfartsselskaber.
98. Den tilsynsførende minder om, at pushmetoden, der giver luftfartsselskaberne mulighed for at holde kontrol med beskaffenheden af de videregivne oplysninger og omstændighederne ved videregivelsen, er den eneste acceptable metode set ud fra et proportionalitetssynspunkt. Desuden skal der være tale om effektivt push, dvs. oplysningerne bør ikke sendes til en dataformidler som bulkdata, men filtreres på allerførste trin af behandlingen. Det er ikke acceptabelt, at ikke-nødvendige oplysninger — og oplysninger, der ikke er omfattet af bilag I til forslaget — videregives til en tredjepart, heller ikke selv om det er meningen, at denne tredjepart straks skal slette oplysningerne.

Dataopbevaring

99. Ifølge artikel 9 i forslaget skal PNR-oplysninger opbevares i fem år og ved udløbet af denne periode i yderligere otte år i en inaktiv database, som der kun bliver begrænset adgang til.

⁽¹⁾ Betragtning 20 og artikel 3, stk. 3 og 5, i forslaget.

⁽²⁾ Jf. i den forbindelse artikel 15, stk. 1, i direktiv 95/46/EF. Direktivet forbyder en sådan edb-behandlet afgørelse i de tilfælde, hvor den pågældende person vil blive berørt af afgørelsen. Hvad angår forslagets kontekst er det sandsynligt, at retshåndhævelsesafgørelser under alle omstændigheder vil berøre de registrerede i væsentlig grad. Det kan også berøre den registrerede at blive underkastet sekundær kontrol, især hvis dette sker gentagne gange.

⁽³⁾ Jf. især udtalelse nr. 5/2007 af 17. august 2007 om opfølgingsaftalen mellem Den Europæiske Union og Amerikas Forenede Stater om luftfartsselskabers behandling og overførsel af passagerliste (PNR)-oplysninger til United States Department of Homeland Security indgået i juli 2007, WP 138.

⁽⁴⁾ Konsekvensanalysen, bilag A (metode til luftfartsselskabernes videregivelse af oplysninger).

100. Den tilsynsførende sætter spørgsmålstegn ved forskellen mellem de to typer databaser: det er tvivlsomt, om den inaktive database udgør et rigtigt arkiv med andre metoder til lagring og fremfindning af oplysninger. De fleste af betingelserne for adgang til den inaktive database består således af sikkerhedskrav, der også kunne gælde for den database, hvor oplysningerne skal opbevares i en femårig periode.

101. Den samlede lagringsperiode — dvs. 13 år — er under alle omstændigheder alt for lang. Den begrundes i konsekvensanalysen med, at den er nødvendig for at udvikle risikoindikatorer og fastslå rejse- og adfærdsmønstre⁽¹⁾, men effektiviteten heraf bør påvises nærmere. Mens det er indlysende, at oplysninger i konkrete tilfælde kan opbevares så længe, der stadig foregår efterforskning, er det ikke berettiget at opbevare oplysninger om alle passagerer i 13 år, uden at der foreligger nogen som helst mistanke.

102. Den tilsynsførende bemærker endvidere, at denne opbevaringsperiode ikke støttes i medlemsstaternes besvarelser af Kommissionens spørgeskema, eftersom den krævede lagringsperiode på grundlag heraf kun ville være på gennemsnitligt 3 1/2 år⁽²⁾.

103. Perioden på 13 år svarer desuden til opbevaringsperioden på 15 år i den seneste aftale med USA. Den tilsynsførende har altid haft den opfattelse, at man kun gik med til denne lange opbevaringsperiode efter kraftigt pres fra den amerikanske regering, der ønskede en meget længere periode end 3 1/2 år, ikke fordi Rådet eller Kommissionen på noget tidspunkt ønskede dette. Der er ingen grund til at overføre et sådant kompromis — der kun skyldes et nødvendigt forhandlingsresultat — til en intern EU-retsakt.

Medlemsstatsudvalgets rolle

104. Det udvalg bestående af medlemsstaterne, der nedsættes i henhold til artikel 14 i forslaget, vil få kompetence med hensyn til sikkerhedsspørgsmål, bl.a. protokoller og kryptering af PNR-oplysninger, men også med hensyn til at fremsætte henstillinger angående fælles generelle kriterier, metoder og praksis for risikovurdering.

105. Bortset herfra indeholder forslaget ingen elementer eller kriterier hvad angår de konkrete betingelser for og rammen om risikovurderingsprocessen. Konsekvensanalysen nævner, at kriterierne i sidste ende vil afhænge af de efterretningsoplysninger, hver medlemsstat er i besiddelse, hvilket konstant skifter. Der vil blive foretaget risikovurdering uden ensartede standarder for identifikation af

mistænkte. Det forekommer derfor tvivlsomt, om medlemsstatsudvalget vil blive i stand til at spille en rolle i den forbindelse.

Sikkerhed

106. Forslaget indeholder en række sikkerhedsforanstaltninger⁽³⁾, der skal træffes af passageroplysningsenhederne, dataformidlerne og de andre kompetente myndigheder med henblik på databeskyttelse. I betragtning af databasens betydning og hvor følsom behandlingen er, finder den tilsynsførende, at ud over de allerede nævnte foranstaltninger bør den enhed, der behandler oplysningerne, også have pligt til at foretage officiel underretning om eventuelle brud på sikkerheden.

107. Den tilsynsførende er klar over, at der er planer om at indføre en sådan underretningsprocedure i sektoren for elektronisk kommunikation på europæisk plan. Han råder til, at der indsættes en sådan sikkerhedsmekanisme i forslaget, og henviser i den forbindelse til den ordning angående brud på sikkerheden, der er indført i USA for officielle organers vedkommende⁽⁴⁾. Sikkerhedshændelser kan nemlig forekomme på alle områder og i den private såvel som den offentlige sektor, hvilket tabet for nylig af en hel borgerdatabase i den britiske offentlige forvaltning har vist⁽⁵⁾. Storstilede databaser som den, der er forudset i forslaget, vil stå øverst på en prioriteret liste med henblik på indførelse af et sådant alarmsystem.

Revisions- og udløbsklausul

108. Den tilsynsførende bemærker, at der skal foretages en fornyet vurdering inden tre år efter rammeafgørelsens ikrafttrædelse på grundlag af en rapport fra Kommissionen. Han noterer sig, at denne fornyede vurdering på grundlag af medlemsstaternes oplysninger vil have særlig fokus på databeskyttelsesgarantier og omfatte gennemførelsen af pushmetoden, dataopbevaringsperioden og kvaliteten af risikovurderingen. For at en sådan fornyet vurdering kan blive dækkende, bør den inkludere resultaterne af en analyse af de statistiske data, der er udarbejdet på grundlag af behandlingen af PNR-oplysninger. Ud over de elementer, der er nævnt i artikel 18 i forslaget, bør disse statistikker også omfatte nærmere statistiske oplysninger om identifikationen af personer, der udgør en stor risiko, såsom kriterierne for sådan identifikation og de konkrete resultater af eventuelle retshåndhævelsesforanstaltninger som følge af identifikationen.

⁽³⁾ Artikel 12 i forslaget.

⁽⁴⁾ Se især arbejdet i den amerikanske Identity Theft Task Force, <http://www.idtheft.gov/>

⁽⁵⁾ Se linket til websiden for British HM Revenue and Customs, <http://www.hmrc.gov.uk/childbenefit/update-faqs.htm>
Se også http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

⁽¹⁾ Konsekvensanalysen, bilag A (dataopbevaringsperiode).

⁽²⁾ Konsekvensanalysen, bilag B.

109. Den tilsynsførende har i denne udtalelse allerede understreget, at der mangler konkrete elementer, der viser, at det foreslåede system er nødvendigt. Han finder dog, at hvis rammeafgørelsen træder i kraft, bør der som minimum indsættes en ophørsklausul. Rammeafgørelsen bør ophæves efter treårsperioden, hvis der ikke kommer noget frem, der støtter dens videre anvendelse.

Følger for andre juridiske instrumenter

110. Forslagets afsluttende bestemmelser indeholder en betingelse for den videre anvendelse af allerede eksisterende bilaterale eller multilaterale aftaler eller ordninger. Disse instrumenter kan kun anvendes, for så vidt som de er forenelige med målene i den foreslåede rammeafgørelse.

111. Den tilsynsførende sætter spørgsmålstegn ved rækkevidden af denne bestemmelse. Som allerede nævnt i kapitel V i afsnittet om gensidighed er det ikke klart, hvad virkningen af denne bestemmelse bliver for indholdet af aftaler med tredjelande som f.eks. aftalen med USA. Set i et andet perspektiv er det heller ikke klart, om bestemmelsen kan få følger for betingelserne for anvendelsen af instrumenter med et bredere anvendelsesområde som f.eks. Europarådets konvention nr. 108. Selv om dette kan forekomme usandsynligt på grund af forskellene i den institutionelle kontekst og de forskellige aktører, der er involveret, bør enhver risiko for fejlfortolkning undgås, og forslaget bør gøre det klart, at det ikke har nogen følger for instrumenter med et bredere anvendelsesområde, især instrumenter, der tager sigte på beskyttelse af de grundlæggende rettigheder.

VII. KONKLUSION

112. Den tilsynsførende understreger, at forslaget har stor betydning for databeskyttelsen. Han har i sin analyse koncentreret sig om fire fundamentale spørgsmål, som forslaget rejser, og insisterer på, at de rejste spørgsmål skal løses på en samlet måde. Under de nuværende omstændigheder er forslaget ikke i overensstemmelse med de grundlæggende rettigheder, særlig artikel 8 i EU-charteret om grundlæggende rettigheder, og det bør derfor ikke vedtages.

113. Hvis der sættes ind i overensstemmelse med ovenstående bemærkninger, især for så vidt angår legitimitetstesten, er der i denne udtalelse fremsat en række formuleringsforslag, som lovgiveren bør tage hensyn til. Der henvises især til punkt 67, 73, 77, 80, 90, 93, 106, 109 og 111 i udtalelsen.

De foreslåede foranstaltningers legitimitet

114. Mens det generelle formål, dvs. at bekæmpe terrorisme og organiseret kriminalitet, i sig selv er klart og legitimt, er kernen i den påtænkte databehandling ikke tilstrækkeligt afgrænset og begrundet.

115. Den tilsynsførende finder, at teknikker, der består i at vurdere den risiko, som enkeltpersoner udgør, ved brug af data mining-redskaber og adfærdsmønstre, skal undersøges nærmere og deres nytte i forbindelse med bekæmpelse af terrorisme klart påvises, før de anvendes i så stort omfang.

116. Det, at man bygger på forskellige databaser uden at have et samlet overblik over de konkrete resultater og mangler:

— er i modstrid med en rationel lovgivningspolitik, hvorefter der ikke må vedtages nye instrumenter, før de eksisterende instrumenter er fuldt gennemført og har vist sig at være utilstrækkelige

— kan betyde et skridt i retning af et fuldstændigt overvågningsfund.

117. Bekæmpelse af terrorisme kan helt sikkert være en legitim grund til at fravige den grundlæggende ret til privatlivets fred og databeskyttelse. Men det er kun legitimt at tilside-sætte disse rettigheder, hvis det påvises klart og ubestrideligt, at dette er nødvendigt, og det skal også påvises, at databehandlingen er i overensstemmelse med proportionalitetsprincippet. Dette er så meget desto mere påkrævet i tilfælde af et så omfattende indgreb i privatlivets fred som det, der er tale om i forslaget.

118. Denne begrundelse mangler i forslaget, og kravet om nødvendigheds- og proportionalitetstest er ikke opfyldt.

119. Den tilsynsførende understreger, at det er af stor vigtighed at foretage nødvendigheds- og proportionalitetstest som nævnt ovenfor. Sådanne test er en absolut betingelse for, at forslaget kan træde i kraft.

Gældende retlig ramme

120. Den tilsynsførende bemærker, at der er alvorlig mangel på retssikkerhed med hensyn til, hvilken ordning der skal gælde for de forskellige aktører, der er involveret i projektet, og især for luftfartsselskaber og andre søjle 1-aktører: det er tilfældet i reglerne i forslaget, i reglerne i rammeafgørelsen om databeskyttelse og i den nationale lovgivning til gennemførelse af direktiv 95/46/EF. Lovgiveren bør gøre det klart, på hvilke trin af behandlingen disse forskellige regler finder anvendelse.

121. Den nuværende tendens til systematisk at pålægge private aktører samarbejde med henblik på retshåndhævelse rejser spørgsmålet om, hvilken databeskyttelsesramme (søjle 1 eller 3) der gælder for betingelserne for dette samarbejde: det er ikke klart, om reglerne bør baseres på beskaffenheden af den dataansvarlige (den private sektor) eller det tilstræbte formål (retshåndhævelse).

122. Den tilsynsførende har allerede fremhævet risikoen for et juridisk tomrum mellem søjle 1- og søjle 3-aktiviteter⁽¹⁾. Det er således langt fra klart, om private selskabers aktiviteter, der på den ene eller den anden måde hænger sammen med håndhævelse af strafferetten, falder ind under området for EU-lovgiverens handling i henhold til artikel 30, 31 og 34 i TEU.
123. Et resultat, der betyder, at tjenesteudbydernes behandling af oplysninger til forskellige formål bliver omfattet af forskellige databeskyttelsesrammer, bør undgås, især i betragtning af de vanskeligheder, som dette vil give anledning til for så vidt angår de registreredes udøvelse af deres rettigheder.

Modtagernes beskaffenhed

124. Forslaget bør give en nærmere præcisering af beskaffenheden af modtagerne af de personoplysninger, luftfartsselskaberne indsamler, og det gælder både dataformidlerne, passageroplysningsenhederne og de kompetente myndigheder.
125. Beskaffenheden af modtageren, der i nogle tilfælde kan være en aktør i den private sektor, hænger direkte sammen med den type databeskyttelsesgarantier, der gælder for den pågældende modtager. Det er væsentligt, at den gældende ordning er klar for alle involverede aktører, herunder lovgiveren og databeskyttelsesmyndighederne, såvel som for de involverede dataansvarlige og registre-rede.

Videregivelse af oplysninger til tredjelande

126. Den tilsynsførende understreger, at det er nødvendigt at sikre et tilstrækkeligt beskyttelsesniveau i modtagerlandet. Han sætter også spørgsmålstegn ved det gensidighedsprincip, der nævnes i forslaget, og dets anvendelse på lande, der allerede er bundet af en aftale med EU såsom Canada og USA. Han anser det for at være af allerstørste vigtighed, at betingelserne for videregivelse af PNR-oplysninger til tredjelande er konsekvente og videregivelsen afhængig af et harmoniseret beskyttelsesniveau.

Andre væsentlige punkter

127. Den tilsynsførende henleder også lovgiverens opmærksomhed på en række specifikke aspekter af forslaget, som kræver nærmere præcisering eller bedre hensyntagen til databeskyttelsesprincippet. Dette er især tilfældet for følgende aspekters vedkommende:
- der bør være strengere betingelser for, hvornår der kan træffes automatiserede afgørelser
 - mængden af behandlede oplysninger bør reduceres
 - oplysninger bør udelukkende videregives efter push-metoden
 - dataopbevaringsperioden er alt for lang og ikke begrundet
 - medlemsstatsudvalgets rolle kunne være mere præcis med hensyn til dets henstillinger angående risikovurdering
 - sikkerhedsforanstaltningerne bør omfatte en procedure for underretning om brud på sikkerheden
 - bestemmelsen om fornyet vurdering af afgørelsen bør omfatte en ophørsklausul
 - forslaget bør gøre det klart, at det ikke har nogen følger for instrumenter med et bredere anvendelsesområde, især instrumenter, der tager sigte på beskyttelse af de grundlæggende rettigheder.

Afsluttende bemærkninger

128. Den tilsynsførende bemærker, at forslaget fremsættes på et tidspunkt, hvor EU's institutionelle kontekst står for at ændre sig fundamentalt. Lissabontraktaten vil få fundamentale følger for beslutningsprocessen, især hvad angår Europa-Parlamentets rolle.
129. I betragtning af de hidtil usete følger, som forslaget vil kunne få for de grundlæggende rettigheder, anbefaler den tilsynsførende, at man ikke vedtager forslaget inden for de nuværende traktatrammer, men sørger for, at det vedtages efter den fælles beslutningsprocedure i den nye traktat. Dette vil styrke retsgrundlaget for vedtagelsen af de afgørende foranstaltninger, der er omhandlet i forslaget.

⁽¹⁾ Jf. udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om opfølgning på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet (EUT C 255 af 27.10.2007, s. 1). Jf. også årsrapporten 2006, s. 47.