Datatilsynet

Samferdselsdepartementet
Postboks 8010 Dep

0030 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
09/585/HK	10/00024-2 /CBR	11. mars 2010

Høringsuttalelse – implementering av datalagringsdirektivet (2006/24/EC)

Del I Innledning og kort oppsummering

Datalagringsdirektivet vil innebære en massiv, statlig innsamling og lagring av opplysninger om hvilke personer som til enhver tid kommuniserer med hverandre ved hjelp av elektroniske hjelpemidler, når denne kommunikasjonen skjer og hvor den enkelte da befinner seg[1]. Opplysningene skal lagres i minst seks måneder.

Datatilsynet mener at dette innebærer en betydelig trussel mot personvernet, både som en individuell rettighet og som et middel for å bevare den tilliten og maktbalansen mellom den norske stat og dens borgere, som er nødvendig i et demokrati[2].

Datatilsynet er ikke alene om å oppfatte datalagringsdirektivet som et forsøk på å institusjonalisere en paternalisme som vil kunne oppfattes som mistillit og urimelig frihetsbegrensning for hele befolkningen. Datatilsynet viser til at også europeiske personvernmyndigheter[3] har uttrykt sterk bekymring for direktivet

Også det faktum at forfatningsdomstolene i Romania og Tyskland har fastslått at direktivet, slik det er implementert i disse landene, er i strid med de nasjonale konstitusjonene viser hvor tett direktivet går de allmenne, demokratiske rettsprinsipper på klingen.

Grunnholdningen som ligger bak kan direktivet karakteriseres som en form for "totalitært svermeri", nemlig en diffus lengsel etter en tilstand der individet er underordnet statens behov for kunnskap om og kontroll med individene. Den bygger på en ubegrunnet forestilling om at alle politiske, sosiale og kulturelle problemer lar seg løse ved storstilet innhenting, lagring, bearbeiding og analyse av personopplysninger. Ettersom teknologien ikke lenger setter grenser for statens muligheter i dette henseende, er det desto viktigere at staten i stedet lar seg begrense av de menneskerettsprinsipper som personvernet representerer.

---

[1] Se pkt 2.1 annet avsnitt
[2] Se pkt 4.4.
[3] European Data Protection Supervisor (EDPS) og Artikkel 29-gruppen

Postadresse: Postboks 8177 Dep 0034 OSLO | Kontoradresse: Tollbugt 3 | Telefon: 22 39 69 00 | Telefaks: 22 42 23 50 | Org.nr: 974 761 467 | Hjemmeside: www.datatilsynet.no

Datatilsynet finner ikke at det er dokumentert i departementenes høringsnotat at datalagringen er så nødvendig for å avdekke, etterforske og rettsforfølge den type kriminaliteten som er foreslått omfattet, at tiltaket til tross for personvernimplikasjonene fremstår å være forholdsmessig[4]. Tilsynet er derfor av den oppfatning at datalagringen strider mot Den europeiske Menneskerettskonvensjon (EMK) artikkel 8, og vil på det sterkeste advare mot at det implementeres i norsk rett.

Det er uansett viktig å ha i mente at EMK artikkel 8 oppstiller et minimumskrav for den enkeltes rett til privatliv. Det er altså ingen ting i veien for at den enkelte medlemsstat sikrer borgerne et bedre personvern enn artikkelen gir anvisning på. Spørsmålet om konvensjonsstrid er altså ikke nødvendigvis avgjørende for spørsmålet om direktivet bør implementeres.

Tilsynet mener at spørsmålet om implementering av datalagringsdirektivet først og fremst er et prinsipielt spørsmål, og at det derfor er av underordnet betydning hvordan direktivet eventuelt implementeres (med tanke på for eksempel lagringstid og -sted). De subsidiære problemstillingene berøres allikevel kort i høringsuttalelsens del V.

Del II Merknader til departementenes utredning

Generelt

I lys av at implementering av direktivet uomtvistelig reiser en rekke vanskelige og problemstillinger, synes Datatilsynet at departementenes utredning er bemerkelsesverdig mangelfull.

Datalagringen må etter tilsynets mening vurderes som et varig tiltak. Det må sies å ha formodningen mot seg at datalagringen, hvis den først blir etablert, vil avvikles innen overskuelig fremtid. Det må tvert imot tas høyde for at ordningen utvikler seg etter implementeringen, for eksempel at opplysningene vil bli bruk til andre formål, at nye opplysningstyper blir omfattet, at lagringstiden endres osv.

Når departementene har forsøkt å utrede konsekvensene av å innføre dette tiltaket har de allikevel tatt utgangspunkt i et "nåtidsvakuum", uten synlige perspektiver på den teknologiske utviklingen, eller den historiske og fremtidige samfunnsutviklingen.

Datatilsynet registrerer blant annet at det ikke er belyst hvordan våre *elektroniske kommunikasjonsmønstre* har endret seg etter at EU vedtok datalagringsdirektivet, og hvordan kommunikasjonsmønstrene vil se vil se ut om kort tid. Tilsynet vil derfor peke på at inntoget av for eksempel smart-telefoner og internettbasert kommunikasjonsutstyr i biler medfører at hver av oss kommuniserer elektronisk på en helt annen måte, og i et stadig større omfang, enn det som var tilfellet når direktivet ble vedtatt.

[4] Se pkt 5

Det er grunn til å tro at de fleste innen kort tid er i besittelse av en smart-telefon. Slike telefoner inneholder applikasjoner som kobler seg automatisk til Internett mange ganger i løpet av et døgn, for å oppdatere opplysninger om været, sportsresultater, motta e-poster osv. Opplysninger om *alle* disse oppkoblingene vil registreres og lagres i medhold av direktivet, herunder vil det lagres opplysninger om hvor telefonen befinner seg når opp- og nedkoblingen skjer. Det samme gjelder for oppkoblinger som gjøres av elektronisk kommunikasjonsutstyr som blir stadig mer vanlig i biler, for eksempel automatisk oppdatering av vei- og værmeldinger via Internett.

Dette innebærer at det ikke bare skal registreres enkelte øyeblikk av våre liv, men at registreringen nærmest blir kontinuerlig. Tilsynet fastholder at en så omfattende statlig registrering av opplysninger om borgerne som det her legges opp til må betegnes som overvåkning[5].

Datatilsynet registrerer at departementene heller ikke har forsøkt å belyse hvilke *nye og gamle metoder* som kan benyttes for å unndra seg den aktuelle registreringen i forbindelse med kriminelle handlinger. Det er etter tilsynets vurdering helt nødvendig at også dette utredes, når nytten av lagringen skal bestemmes. Herunder må det også utredes hvordan man vil møte en slik utfordring. Datatilsynet frykter at man fort vil se nødvendigheten av for eksempel å lagre innholdsdata for Internettsurfing, for å kunne registrere e-post sendt og mottatt via Internett-mail[6], og av innholdsdata fra telefonsamtaler for å verifisere hvem som faktisk har benyttet en påstått stjålet telefon. Man må være klar over faren for å havne i en "kontrollspiral", hvor stadig mer inngripende tiltak blir nødvendige fordi gamle tiltak mister sin effekt.

Datatilsynet mener at utredningen også mangler perspektiver om *den historiske og den fremtidige samfunnsutviklingen.* Selv om dagens regjering har en sterk demokratisk forankring, og stiller garantier for at de ikke vil misbruke disse opplysningene, er det allikevel nødvendig å belyse hvilke store muligheter datalagringen *som sådan* gir for myndighetsmisbruk. I en ansvarlig utredning bør det reflekteres over at det faktisk er uklart hvem som i fremtiden skal besitte det verktøyet som datalagringen representerer.

Kort om gjeldende sletteplikt for IP-adresser

I debatten omkring datalagringsdirektivet er Datatilsynets vedtak overfor flere Internettleverandører blitt brukt som begrunnelse for hvorfor direktivet er nødvendig. Datatilsynet kritiseres for ikke å ha tatt høyde for politiets behov, når det er besluttet at koblingen mellom person og IP-adresse skal slettes etter tre uker.

Datatilsynet vil benytte anledningen til å presisere følgende: Det er leverandørene som er behandlingsansvarlige for nevnte opplysninger i henhold til personopplysningsloven. Det innebærer at det er *leverandørenes* formål som er styrende for om opplysningene kan behandles, hvordan de kan behandles og når de skal slettes i henhold til personopplysningslovens bestemmelser.

---

[5] "En stadig iakttakelse, observasjon, oppsikt" (Bokmålsordboka ,2008)
[6] Se pkt 2.5

Leverandørene har selvsagt ikke et politimessig formål for sin virksomhet, og har opplyst at de behandler opplysningene for det formål å sikre en forsvarlig drift av sine tjenester. Det følger av dette at leverandørene som hovedregel skal slette disse opplysningene når deres eget formål er opphørt. I dette tilfelle vil det si omtrent etter tre uker.

Hvilket formål *politiet* eventuelt kan bruke opplysningene til er altså irrelevant i denne forbindelse. Dersom Datatilsynet hadde sett hen til politiets behov for data ved fastsettelsen av leverandørenes lagringstid ville tilsynet tatt utenforliggende hensyn. Det er under enhver omstendighet lovgiver som skal regulere politiets behandling av personopplysninger i forbindelse med etterforskning av straffbare handlinger.

Frikjennelsesbegrunnelsen

Datatilsynet reagerer på at departementene begrunner datalagringen med at opplysningene vil være nødvendige for å *frikjenne* noen som er urettmessig mistenkt for alvorlig kriminalitet[7]. Tilsynet skal i den forbindelse bemerke at det er en lang og god norsk strafferettstradisjon for prinsippet om at en borger er å anse som uskyldig inntil det motsatte er bevist utenfor rimelig tvil – den såkalte *uskyldspresumpsjonen*. Samme prinsipp er nedfelt i Den europeiske Menneskerettskonvensjon art 6.

Det er altså borgerens skyld som skal bevises, ikke hans uskyld. Departementenes argumentasjon om at datalagringen også er nødvendig for å frikjenne de som er uskyldige rokker etter tilsynets vurdering ved dette grunnleggende prinsippet, og er derfor svært uheldig.

Bruk av opplysningene til sivile formål

Datatilsynet beklager at departementene ikke belyser i hvilken grad opplysninger fra tilbyderne, når de først er lagret i henhold til datalagringsdirektivet, kan kreves utlevert for sivile formål, for eksempel av norske domstoler utover straffesaksbehandlingen. Dette forholdet er selvsagt relevant for å belyse hvordan angjeldende opplysninger vil tilflyte samfunnet, og derved identifisere ulempene for personvernet.

Forholdet til kommunikasjonskontroll

Datatilsynet reagerer på at departementene sammenligner datalagringen med kommunikasjonskontroll, når de forsøker å imøtegå påstanden om at datalagringen er inngripende[8]. Det at datalagringen er "mindre inngripende" enn for eksempel telefonavlytting er i beste fall irrelevant.

I motsetning til datalagring er kommunikasjonskontroll en *målrettet* metode som kan tas i bruk overfor en *begrenset krets* med personer når det foreligger *kvalifisert mistanke* om særlig grove lovbrudd, jf straffeprosessloven kapittel 16a.

[7] høringsnotatet pkt 4.1
[8] høringsnotatet pkt 4.2

Datalagringen er imidlertid et tiltak som iverksettes *uten* at det foreligger noen konkret mistanke mot noen, og som retter seg mot *hele befolkningen*. Det er etter tilsynets mening åpenbart at dette er to metoder som er grunnleggende ulike, og derfor ikke kan sammenlignes med hverandre.

Innholdsdata og trafikkdata

Direktivet omfatter lagring av trafikkdata, men ikke innholdsdata. Datatilsynet stiller imidlertid spørsmål ved om det faktisk er mulig å lagre trafikkdata om e-post som sendes og mottas via en Internettbasert e-posttjeneste (type g-mail), derom det ikke skal registreres innholdsdata vedrørende Internettbruk (hvilke internettsider man har besøkt).

Dersom departementene er av den oppfatning at også slike e-poster uansett skal registreres, må det nødvendigvis åpnes for registrering av innholdsdata. Kommer departementene til at denne type e-post likevel må forbli uregistrert, så etableres det en enkel og stor mulighet for å omgå datalagringen. Dette undergraver nødvendigheten av lagringen som sådan.

Datatilsynet savner en klargjøring av dette punktet.

Utlevering og tilgang

Datatilsynet vil understreke at det er en prinsipiell forskjell på det å gi politiet *"tilgang til"* opplysningene hos teleselskapene og det at politiet skal kunne få opplysningene *"utlevert"* fra teleselskapene.

Mens tilgang kan ses som en mulighet til selvbetjening av opplysninger, nødvendiggjør en utlevering at avgiver foretar en konkret vurdering av om vilkårene for utlevering er tilstede i ethvert tilfelle.

At disse begrepene usystematisk benyttes om hverandre i departementenes utredning, kan medføre misforståelser. Det bør klargjøres hvordan opplysningene rent praktisk skal tilflyte politiet fra teleselskapene.

Del III Er datalagringen nødvendig for at staten skal kunne ivareta sine forpliktelser etter EMK art 8?

Det er i debatten om direktivet hevdet at datalagringen er nødvendig for at Norge skal oppfylle sine forpliktelser etter Den europeiske Menneskerettskonvensjon artikkel 8. Det er i den forbindelse vist til en dom avsagt av Den europeiske menneskerettsdomstol den 2. desember 2008, *KU vs Finland* (2872/02).

I denne saken ble Finland dømt for brudd på EMK artikkel 8, idet staten ikke hadde lagt til rette for at det var mulig å etterforske et tilfelle hvor noen hadde lagt ut sensitive opplysninger om en 12 år gammel gutt på Internett, og derved krenket hans personvern. Etterforskningen ble umuliggjort fordi teleselskapenes lovhjemlede taushetsplikt var til hinder for at eksisterende trafikkdata kunne leveres ut til politi og påtalemyndighet.

Menneskerettsdomstolen mente at rettstilstanden ikke tilfredsstillende balanserte hensynet til telekundenes krav på personvern mot hensynet til en effektiv straffeforfølgning av brudd på personvernet.

I den norske debatten om datalagringsdirektivet er dommen tatt til inntekt for at staten nærmest er forpliktet til å registrere og oppbevare trafikkopplysninger, uavhengig av datalagringsdirektivet.

Datatilsynet mener at det er å trekke dommen altfor langt. Menneskerettsdomstolen har ikke tatt stilling til *lagringsspørsmålet*, dvs hvorvidt trafikkdata skal registreres og lagres. Domstolen har bare vurdert *utleveringsspørsmålet,* dvs i hvilken grad de trafikkdata som faktisk er lagret skal kunne utleveres til politi og påtalemyndighet.

Del IV Er datalagringen forholdsmessig, jf EMK art 8?

Generelt

I henhold til Den europeiske menneskerettskonvensjon (EMK) artikkel 8, kan et tiltak som griper inn i personvernet bare gjennomføres dersom tiltaket "er nødvendig i en demokratisk rettsstat".

Identifisering av tiltaket

Datatilsynet vil understreke at forholdsmessighetsvurderingen må knyttes til *innsamlingen og lagringen* av de aktuelle opplysningene, ikke til den senere *utleveringen.* Det er altså ulempen og nytten av at staten registrerer og lagrer en rekke opplysninger om enhver som benytter elektroniske kommunikasjonsmidler, som må identifiseres og avveies.

Den forholdsmessighetsvurderingen som domstolen skal foreta gjelder utlevering av de opplysningene som allerede er lagret. Hvorvidt den forutgående innsamling og lagring er forholdsmessig, er altså et spørsmål som lovgiver må ta selvstendig stilling til.

Er registrering og lagring av trafikkdata nødvendig for å nå formålet?

EMK artikkel 8 annet ledd krever at et tiltak som griper inn i personvernet bare kan iverksettes når det er "nødvendig". Det følger av Menneskerettdomstolens praksis at dette er et krav om at det må foreligge et tvingende samfunnsmessig behov for tiltaket.

Datatilsynet vil bemerke at departementenes utredning er mangelfull også på dette punktet. Det opplyses at "Departementene har vurdert problemstillingen, og kan ikke se at det finnes alternativ som kan erstatte datas betydning i etterforskningen av alvorlig kriminalitet"[9]. Departementene går imidlertid ikke nærmere inn på hvilke vurderinger som er gjort.

En vurdering av hvilke opplysninger som er nødvendige for politi og påtalemyndighet i forbindelse med å avdekke, etterforske og rettsforfølge alvorlig kriminalitet vil langt på vei

[9] jf høringsnotatet s 29

måtte bero på et *politifaglig skjønn*. Datatilsynet mangler realkompetanse til å kunne foreta den type vurderinger, men forventer at den nødvendighetsvurderingen som skal ligge til grunn for Stortinget forholdsmessighetsvurdering er forsvarlig og dokumentert.

Da tilsynet ikke ser at departementenes utredning tilfredsstiller disse kravene, har tilsynet tatt initiativ til et eget utredningsarbeid for å belyse nødvendigheten. Tilsynets rapport fra dette arbeidet vil ettersendes så snart den er ferdig.

Behov for konkretisering

Datatilsynet vil bemerke at enhver personopplysning potensielt vil kunne være nødvendig i forbindelse med forebygging og etterforskning av alvorlige straffbare forhold. Det gjelder imidlertid ikke bare de trafikkdata som direktivet omhandler, men også for eksempel trafikkdata fra bomstasjoner og offentlige transportmidler, samt opplysninger om økonomiske transaksjoner, opptak fra fjernsynsovervåkningskameraer, helseopplysninger og diverse annet.

En forsvarlig nødvendighetsvurdering må derfor være så konkret som mulig. Nødvendigheten av de konkrete personopplysninger som det her er tale om må altså vurderes opp mot det konkrete formålet, nemlig å avdekke, etterforske og rettsforfølge de straffbare handlinger som foreslås omfattet av direktivets virkeområde.

Den nødvendighetsvurdering som departementene har foretatt, er etter tilsynets vurdering så generell og "sjablongmessig" at den ikke er forsvarlig og derfor ikke bør legges til grunn for Stortingets forholdsmessighetsvurdering.

Tiltakets effektivitet

Når det skal vurderes hvorvidt et tiltak er nødvendig, er det et sentralt moment hvorvidt tiltaket er effektivt for å nå det konkrete formål.

Dersom et kontrolltiltak er lett å omgå, vil det neppe være egnet til å nå formålet med tiltaket, og kan derfor heller ikke kunne sies å være nødvendig. Det må derfor klarlegges hvorvidt, og eventuelt hvor enkelt, lovbryterne vil kunne *unndra seg den registreringen* som datalagringsdirektivet omhandler.

Datatilsynet mener også her at departementenes utredning er mangelfull, idet det ikke tas høyde for at lovbryterne kan unndra seg datalagringen ved bruk av for eksempel Internett-cafeer, usikrede trådløse nettverk, stjålne mobiltelefoner og fremtidig teknologi.

Det har vært gjort ulike forsøk på å *tallfeste effekten* av datalagringen. Det har for eksempel blitt hevdet at denne type opplysningene har vært nyttige i ca 45 % av alle saker hvor opplysningene har vært innhentet av politiet. Datatilsynet mener at en slik tilnærming er meningsløs. Dersom trafikkdataene kunne blitt brukt til enhver politioppgave hadde selvsagt den andelen av de lagrede opplysningene som hadde kommet til nytte ha vært enda større.

Videre skal det pekes på at tallfestingen bygger på erfaringer gjort før datalagringen er et faktum. Det er imidlertid grunn til å tro at datalagringen vil medføre endringer i lovbryternes adferd, i den forstand at de velger alternative, "sikrere" metoder.

Det er etter dette høyst usikkert hvor effektiv datalagringen vil være for å avdekke, etterforske og rettsforfølge de straffbare forhold som er foreslått omfattet.

Alternative tiltak

Når det skal vurderes hvorvidt et tiltak er nødvendig, må det også belyses hvilke alternative tiltak som eventuelt kan brukes for å nå det aktuelle formålet, eventuelt må det begrunnes hvorfor de alternative metodene ikke fungerer tilfredsstillende. Datatilsynet kan ikke se at departementene har gjort en slik vurdering i dette tilfellet.

Medfører datalagringen ulemper for personvernet?

Mange vil hevde at den *faktiske* endringen ved å implementere direktivet ikke er dramatisk, da flere av de opplysningene som direktivet omhandler registreres av teleselskapene også i dag, og lagres der i inntil fem måneder. *Rettslig og prinsipielt* medfører imidlertid en eventuell implementering en dramatisk endring.

Opplysningenes art og omfang

Det kan generelt hevdes at jo flere personopplysninger som behandles, og jo mer sensitive opplysningene er, desto større er ulempen for personvernet.

Datalagringsdirektivet medfører i utgangspunktet ingen behandling av *sensitive* personopplysninger, slik de er definert i EUs personverndirektiv og personopplysningslovens § 2 nr 8. Det kan imidlertid ikke være tvil om at de opplysningene som skal lagres, over tid og samlet, vil kunne være egnet til å si noe om den enkeltes sensitive forhold, herunder ens legning, religion, helseforhold og politisk oppfatning.

Datalagringsdirektivet medfører uansett at de opplysningene som skal registreres om den enkelte er *svært omfattende,* og lett vil kunne gi grunnlag for å utarbeide såkalte sosiogrammer.

Formålet med lagringen

I en rettsstat må det finnes klare grenser for hvilke tiltak staten kan iverksette med tanke på å forebygge og etterforske straffbare forhold.

Dagens rettstilstand gjenspeiler dette. Det kan ikke iverksettes *etterforskning*, med mindre det som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige, jf strpl § 224.

Dersom tiltaket retter seg mot en konkret person kreves det i tillegg at det foreligger er en kvalifisert mistanke mot vedkommende. Vilkårene er enda strengere når formålet med tiltaket er å *avverge* straffbare handlinger. Det kan ikke iverksettes målrettede tiltak for å forebygge

straffbare handlinger, med mindre det er rimelig grunn til å tro at noen kommer til å begå bestemt angitte lovbrudd.

Datatilsynet mener datalagringen i henhold til direktivet kan ses som en *forskuttert etterforskningsmetode*, som skal kunne tas i bruk før gjeldende vilkår for å ta i bruk ordinære metoder er oppfylt.

At staten iverksetter etterforskningstiltak som retter seg mot hele samfunnet, uten at det foreligger mistanke mot noen, og før det engang er identifisert et mulig lovbrudd, innebærer et paradigmeskifte i norsk strafferettstradisjon og kan ses som et uttrykk for at hele folket settes under mistanke.

Selvbestemmelsesrett

Den enkeltes selvbestemmelsesrett er et helt grunnleggende personvernprinsipp; enhver skal i utgangspunktet ha rett til å bestemme over sine egne personopplysninger, med tanke på hvem som behandler dem, til hvilke formål de benyttes osv. Dette utgangspunktet gjelder uavhengig av om opplysningene er sensitive eller ikke.

I dag behandler teleselskapene disse opplysningene med hjemmel i en privatrettslig avtale som er frivillig inngått mellom selskapet og dets kunder. I henhold til datalagringsdirektivet skal opplysningene i stedet lagres med hjemmel i et lovpålegg overfor teleselskapene. Dette betyr at individet gjennom direktivet fratas den råderetten han i dag har over disse opplysningene. Det representerer et klart brudd på den enkeltes personvern.

Datatilsynet vil i den forbindelse bemerke at det å avstå fra å bruke elektroniske kommunikasjonsformer, for å bevare kontrollen over egne opplysninger, ikke er et praktisk alternativ i dagens samfunn.

Rett til anonym ferdsel

Mange vil hevde at retten til anonym ferdsel er en del av personvernet. Denne kan formuleres som den enkeltes rett til å bevege seg fritt i samfunnet, uten plikt til å legitimere seg eller la seg identifisere.

Datalagringsdirektivet vil langt på vei medføre en løpende registrering av hvor den enkelte befinner seg rent fysisk, nærmest til enhver tid[10]. Slik sett vil datalagringen utfordre retten til anonym ferdsel.

Det samlede overvåkningsnivået

Selv om ett enkelt tiltak ikke skader personvernet i betydelig grad, må det tas høyde for at den samlede overvåkningen i samfunnet vil kunne havne på et nivå som er skadelig. Når det skal vurderes hvilken virkning det enkelte tiltaket har for personvernet, må det derfor tas utgangspunkt i hvor omfattende overvåkningen er totalt sett.

[10] jf pkt 2.1 annet avsnitt

Det bør være kjent at Datatilsynet allerede er bekymret for omfanget av og vilkårene for den behandlingen av personopplysninger som staten gjennomfører pr i dag. Tilsynet er av den oppfatning at man hurtig nærmer seg en absolutt smertegrense for hva demokratiet kan tåle. Det vil være for langt å gå i detaljer her. Interessenter henvises til den generelle samfunnsdebatten og tilsynets egne publikasjoner, for eksempel dets årsmeldinger.

Når det samlede overvåkningsnivå skal identifiseres kan man imidlertid ikke bare se hen til hvilke tiltak som allerede *er iverksatt*, men også hvilke som med en viss grad av sikkerhet *vil bli iverksatt* i overskuelig tid. Et slags "føre var"-prinsipp tilsier at listen for å iverksette et tiltak ikke kan legges for lavt, da det vil medføre at mange senere tiltak vil kunne bli ansett for å være like nødvendige. Konsekvensen kan bli at den samlede overvåkningen utvikler seg til å bli massiv.

Når det gjelder datalagringsdirektivet må man ha i mente at det er ikke slik at hvis bare politiet får tilgang til de trafikkdata som direktivet omhandler, så vil behovet for andre opplysninger forsvinne. Hvis man finner at lagring av denne type trafikkdata er nødvendig, mener tilsynet at man raskt vil komme til at andre tiltak er like nødvendige. Man legger altså listen for lavt, med tanke på fremtidige tiltak.

Rett til frihet fra statlige myndigheter

Datatilsynet vil minne om at et demokrati kjennetegnes ved at det er borgerne som kontrollerer staten, og ikke motsatt. Det er derfor helt nødvendig å sikre maktbalansen mellom borgerne og staten.

I den forbindelse er et sentralt poeng at innsamling og lagring i henhold til datalagringsdirektivet skjer *i statlig regi*, gjennom et absolutt lovpålegg. Staten gis gjennom datalagringen et maktmiddel, som bidrar til å forrykke balansen mellom stat og individ, og medfører derfor et klart brudd på personvernet. Ved endrede samfunnsforhold vil en slik forskyvning kunne få dramatiske konsekvenser.

Forbud mot overskuddsinformasjon

Forbud mot bruk av overskuddsinformasjon er et grunnleggende personvernprinsipp. Det er altså forbudt å behandle andre eller flere personopplysninger enn det som er nødvendig for å nå formålet med behandlingen.

Selv om det er umulig å tallfeste nytten av datalagringen, så er det liten tvil om at det aller meste av det som skal lagres i henhold til direktivet vil være å anse som overskuddsinformasjon. For det første vil personkretsen som omfattes av lagringen være klart større enn den personkretsen som faktisk gjennomfører slike lovbrudd som det her er tale om. Videre vil det lagres opplysninger som etter sin art og innhold ikke kan knyttes til pågående eller fremtidig kriminalitet.

Datalagringsdirektivet setter innsamling av overskuddsinformasjon i system, og innebærer derfor et klart brudd på personvernet.

Fremtidig utvidelse av bruken

Selv om det er sagt uttrykkelig, både i direktivet og i departementenes utredning, at formålet med datalagringen er å avdekke, etterforske og rettsforfølge alvorlig kriminalitet, må det tas høyde for at dette utgangspunktet vil bli kraftig utfordret. Det er ingen naturlov som skal etableres.

Ut fra den tanke at "det er meningsløst ikke å benytte opplysninger som allerede eksisterer", er det tilsynets erfaring at terskelen for å tillate at opplysninger som er samlet inn for ett formål også brukes til andre formål er svært lav. Tilsynet vil for eksempel minne om at ligningsmyndighetene har fått lovhjemlet adgang til opplysninger fra bompengeselskapene, til tross for at disse var lagret for det formål å fakturere bileiere som passerte bomringen. Tilsynet vil også peke på at EURODAC, som ble opprettet med det formål å identifisere asylsøkere, har blitt tatt i bruk også for politiformål (etterforskning).

De gode formålene, hvor nettopp denne type opplysninger kan være betydningsfulle, står i kø. Det er nok her å nevne forskningsformål og offentlige kontrollformål (for eksempel lignings- og tollmyndigheter), og ikke minst forebygging og etterforskning av andre typer kriminalitet enn det som er foreslått pr i dag (lavere terskel). Datatilsynet er derfor overbevist om at det vil finne sted en såkalt formålsglidning, dersom datalagringen først implementeres.

Det er ikke gitt at disse fremtidige endringene isolert sett vil være store. Samlet sett vil utviklingen likevel kunne være dramatisk.

En formålsglidning vil kunne medføre at opplysningene spres i samfunnet på en helt annen måte enn forutsatt. Det er derfor nødvendig å ta høyde for formålsglidningen, når man skal identifisere hvilke konsekvenser datalagringen vil kunne få for personvernet på sikt.

Datatilsynet kan ikke se at departementene har tatt tilstrekkelig høyde for en slik utvikling.

Avveining mellom fordeler og ulemper ved datalagringen

Den sjablonmessige tilnærmingen departementene har for sin nødvendighetsvurdering, hvor man likestiller alle straffebud med en minimum strafferamme på tre år, er ikke forsvarlig.

Det må kunne forventes en mer konkret vurdering av behovet for *de ulike trafikkopplysningene* knyttet til hvert av *de ulike lovbrudd* som foreslås omfattet. For mens det er nokså klart at opplysninger om hvilke personer som er knyttet til ulike IP-adresser vil kunne ha avgjørende betydning når politiet skal etterforske spredning av barneporno, kan ikke Datatilsynet se at det er dokumentert å være like nødvendig å fremskaffe lokasjonsdata ved bruk av mobiltelefon for å etterforske brudd på straffelovens § 156 om grovt underslag.

Datatilsynet er av den oppfatning at det finnes metoder for å relativt enkelt kunne omgå den registreringen som direktivet foreskriver. Tilsynet savner en analyse av hvilken effekt datalagringen vil få i forbindelse med etterforskning av de ulike kriminelle handlinger, hvor det også tas høyde for at de kriminelles adferd og modus vil endres etter en eventuell implementering. Før en slik analyse foreligger kan det ikke legges til grunn at tiltaket er effektivt.

Datatilsynet kan etter dette ikke se at det er dokumentert i høringsnotatet at det er nødvendig å lagre alle de opplysningene som er foreslått i direktivet, for å etterforske alle de lovbrudd som er foreslått omfattet.

Selv om de lovbrudd hvor opplysningene kan sies å ha en dokumentert nødvendighet er av svært alvorlig karakter, kan disse etter tilsynets vurdering ikke alene forsvare det massive innhugget som lagringen medfører i personvernet.

Datatilsynet har derfor kommet til at datalagringen ikke er dokumentert å være forholdsmessig i henhold til EMK artikkel 8, og at det uansett ikke bør implementeres av de sterke hensyn som ligger bak artikkelen.

Da datalagringen i tillegg utfordrer ytringsfriheten, forsamlings- og foreningsfriheten og muligheten til å gjennomføre anonym varsling og kildevern, og derfor kan virke hemmende for adferd som er å anse som både lovlig og samfunnstjenlig[11], kan ikke Datatilsynet annet enn å advare sterkt mot at direktivet implementeres.

Del V Ivaretakelse av personvernet ved eventuell implementering

Som det fremgår av dette dokumentet anser Datatilsynet at en eventuell implementering av datalagringsdirektivet *som sådan* kommer i konflikt med grunnleggende personvernhensyn.

Dette gjelder altså *uavhengig av hvordan direktivet implementeres*, og hvilke garantier som eventuelt stilles for behandlingen av opplysningene. Tilsynet er derfor av den oppfatning at direktivet ikke kan eller bør implementeres.

Personopplysningslovens anvendelse

Datatilsynet har fått signaler om at det kan bli aktuelt å lovfeste en rekke unntak fra behandlingsreglene i personopplysningsloven, for *tilbydernes* behandling av trafikkopplysningene. Konkret gjelder dette unntak fra den registreres rett til innsyn.

Datatilsynet vil advare mot et slikt unntak. Det å nekte den enkelte borger tilgang til opplysninger som staten har registrert om vedkommende medfører et klart brudd på sentrale rettssikkerhetsgarantier, og gjenspeiler en maktbalanse mellom stat og individ som ikke er et demokrati verdig.

Datatilsynet vil uansett understreke behovet å klargjøre hvorvidt og i hvilken utstrekning personopplysningslovens bestemmelser kommer til anvendelse på leverandørenes behandling av trafikkdataene ved en eventuell implementering. Behovet for eventuelle unntak fra personopplysningsloven må uansett identifiseres og utredes *før* direktivet legges frem for Stortinget, slik at de folkevalgte settes i stand til å ta en informert beslutning.

[11] Lambrinidis rapport (behandlet av Europaparlamentet i 2009 – 2008/2160INI)

Andre vilkår for implementeringen
Departementene har stilt en rekke konkrete spørsmål i sitt høringsnotat, vedrørende de nærmere vilkår for implementering.

Datatilsynet nøyer seg i denne omgang med å vise til vedlagte uttalelser fra de europeiske personvernmyndighetene[12]. Her er forholdet mellom datalagringsdirektivet og personvern utførlig behandlet. Blant annet har man oppstilt konkrete krav til sikkerhetsforanstaltninger for datalagringen. Det er Datatilsynets vurdering at disse må legges til grunn for en eventuell implementering.

Datatilsynet har vedlagt denne lille historien, for å belyse hvor viktig og vanskelig det er å skjelne mellom innbilt og reell trygghet:

Forsikring

"Min uro økte etter hvert som jeg nærmet meg det stedet der skogen var som mørkest. Det ble sagt at noen banditter holdt til der.

Jeg hadde nettopp passert det farlige stedet, da tre stykker kom ut i veien.
- Er dere banditter? spurte jeg.
- Vi? Hvordan kan du tro noe slikt? Vi er skogvoktere.
Jeg pustet lettet ut.

- Men siden du er inne på det, så er det litt av hvert som holder til her. Vi foreslår at du gir oss det du har av kontanter, så kan vi ta vare på det for deg. Innen vits i å ta noen sjanser.

Jeg ga dem alt jeg hadde med meg, så gikk jeg bekymringsløst videre. Det var forresten ingen som antastet meg, ikke spor av banditter. Men så er jeg da også forsiktig av meg."

Sławomir Mrozek (Livet for nybegynnere, Bazar forlag 2007)

Med hilsen

Georg Apenes
Direktør

Cecilie L. B. Rønnevik
seniorrådgiver

Kopi: Fornyings- og Administrasjonsdepartementet, v/Statsforvaltningsavdelingen, Pb 8004 Dep, 0030 Oslo
Vedlegg: Uttalelser fra EDPS og fra Art 29-gruppen

[12] EDPS uttalelse (2005/c 298/01), Art 29-gruppen (4/2005)

Artikel 29-gruppen vedrørende databeskyttelse

1868/05/DA
WP 113

Udtalelse 4/2005 om forslag til Europa-Parlamentets og Rådets direktiv om lagring af data behandlet i forbindelse med tilvejebringelse af offentlige elektroniske kommunikationstjenester og om ændring af direktiv 2002/58/EF (KOM(2005) 438 endelig af 21. september 2005)

Vedtaget den 21. oktober 2005

Denne gruppe er oprettet i henhold til artikel 29 i direktiv 95/46/EF. Den er et uafhængigt europæisk rådgivende organ vedrørende databeskyttelse og privatliv. Dens opgaver er beskrevet i artikel 30 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF.

Gruppens sekretariat: Europa-Kommissionen; GD for Retfærdighed, Frihed og Sikkerhed; Direktorat C - Civilret, grundlæggende rettigheder og EU-borgerskab, B-1049 Bruxelles, Belgien, Kontor LX-46 01/43.

Website: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

RESUMÉ

Europa-Kommissionens forslag til direktiv om lagring af data stiller os over for en historisk beslutning.

Lagring af trafikdata griber ind i den ukrænkelige, grundlæggende rettighed til fortrolig kommunikation.

Enhver begrænsning af denne grundlæggende rettighed skal være baseret på et midlertidig behov, må kun tillades i exceptionelle tilfælde og være omfattet af passende sikkerhedsforanstaltninger.

Udbydere af offentlige kommunikationstjenester vil for første gang af efterforskningshensyn blive tvunget til at lagre enorme mængder data om enhver borgers kommunikation.

Terrorisme stiller vort samfund over for en reel og presserende udfordring. Regeringerne må tage denne udfordring op på en måde, der effektivt dækker borgernes behov for at leve i fred og sikkerhed uden at undergrave deres individuelle menneskerettigheder – herunder retten til datahemmelighed – som er en af vort demokratiske samfunds grundpiller.

Europa-Kommissionens initiativ kan i sidste ende føre til maksimale lagringsperioder, som er kortere end de perioder, der er påregnet i andre af den senere tids forslag.

Gruppen stiller spørgsmålstegn ved, om kravet om obligatorisk og generel lagring af data fra de kompetente myndigheder i medlemsstaterne er baseret på krystalklare beviser. Gruppen er heller ikke overbevist om, at de lagringsperioder, der foreslås i direktivforslaget, er de rette.

Som nævnt skal det klart påvises og dokumenteres, at kravet om obligatorisk og generel datalagring er begrundet. Det gælder også de maksimale lagringsperioder, der skal gælde. Under alle omstændigheder skal det også fremgå helt tydeligt, under hvilke betingelser de kompetente myndigheder kan få adgang til og benytte sådanne data til bekæmpelse af truslen om terrorisme.

Formålet med lagring af data skal fremgå tydeligt af direktivet med en henvisning til bekæmpelse af terrorisme og organiseret kriminalitet frem for det ubestemte "grov kriminalitet".

Der skal tages hensyn til, at der findes fremgangsmåder, som i mindre grad krænker privatlivet (f.eks. quick-freeze-proceduren).

En eventuel lagringsperiode skal være så kort som muligt og udgøre det maksimale tidsrum for lagring for alle medlemsstaterne, selv om de frit skal kunne fastlægge kortere lagringsperioder. Eventuelle foranstaltninger skal bekendtgøres bredt.

Begrundelsen for disse foranstaltninger skal gennemgås regelmæssigt. De påtænkte foranstaltninger om lagring af data skal være tidsbegrænsede efter begrebet "sunset legislation" (solnedgangslovgivning) og baseres på periodiske evalueringer, der foretages mindst hvert andet eller tredje år og offentliggøres. En treårig periode forekommer passende.

Under alle omstændigheder kan man ikke inden for de eksisterende EU-bestemmelser acceptere at pålægge udbydere af kommunikationstjenester de nævnte forpligtelser til lagring af data uden først at indføre passende, specifikke sikkerhedsforanstaltninger.

Endelig opstillede gruppen 20 specifikke sikkerhedsforanstaltninger, som skal indføres under særlig hensyntagen til kravene til modtagere og viderebehandling, behovet for tilladelser og kontrol, foranstaltninger for tjenesteudbydere også med hensyn til sikkerhed og logisk adskillelse af dataene, fastsættelse af de relevante datakategorier og opdateringer heraf samt behovet for at udelukke indholdsdata.

GRUPPEN VEDRØRENDE BESKYTTELSE AF FYSISKE PERSONER I FORBINDELSE MED BEHANDLING AF PERSONOPLYSNINGER

som er nedsat ved Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995,

har under henvisning til dette direktivs artikel 29, og artikel 30, stk. 1, litra a) og stk. 3, og til artikel 15, stk. 3, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002, og

under henvisning til gruppens forretningsorden, særlig artikel 12 og 14 -

VEDTAGET FØLGENDE UDTALELSE:

I. Baggrund

Som led i de europæiske initiativer til bekæmpelse af terrorisme og organiseret kriminalitet forelagde Kommissionen den 21. september 2005 et "*forslag til direktiv om lagring af data behandlet i forbindelse med tilvejebringelse af offentlige elektroniske kommunikationstjenester og om ændring af direktiv 2002/58/EF*[1]".

Der er tale om et emne af væsentlig betydning for alle borgere.

Frihed, brevhemmelighed og fortrolighed i forbindelse med alle andre former for kommunikation er nogle af grundpillerne for moderne demokratiske samfund. Deres ukrænkelighed er fremhævet i en række akter, herunder forfatningschartre, og indgår specifikt i den europæiske menneskerettighedskonvention, som danner grundlag for fællesskabsretten.

Direktivforslaget stiller os over for en historisk beslutning. Målet er for første gang at indføre en forpligtelse i hele EU til med henblik på efterforskning at lagre enorme mængder data om alle borgeres kommunikation. I henhold til fællesskabsretten lagres sådanne data ikke i øjeblikket, eller også lagres de kun midlertidigt af udbyderne af elektroniske kommunikationstjenester – og når det sker, er det udelukkende af kontraktmæssige hensyn.

Lagring af trafikdata krænker den grundlæggende rettighed til fortrolig kommunikation, som den enkelte er garanteret i den europæiske menneskerettighedskonventions artikel 8. I et demokratisk samfund kan denne grundlæggende ret kun begrænses, hvis det er nødvendigt af hensyn til den nationale sikkerhed. Det kan i yderste konsekvens betyde overvågning og registrering af alle kontakter til og alle forbindelser med fysiske personer samt de steder, hvor dette foregår, og de kommunikationsmidler, der benyttes. Den Europæiske Menneskerettighedsdomstol har endvidere understreget, at hemmelig overvågning rummer en fare for at undergrave eller endog ødelægge demokratiet i forsøget på at forsvare det. Domstolen har desuden fastslået, at stater ikke kan indføre hvilke som helst foranstaltninger, de finder passende, under henvisning til bekæmpelse af spionage og terrorisme[2].

Derfor skal enhver begrænsning af denne grundlæggende rettighed være baseret på et midlertidig behov, den må kun tillades i exceptionelle tilfælde og skal være omfattet af passende

[1] [KOM (2005) 438 endelig], 21.9.2005, *endnu ikke offentliggjort i EUT.*

[2] Klass m.fl. mod Tyskland, præmis 49.

sikkerhedsforanstaltninger. Lagring af trafikdata - herunder lokaliseringsdata – af hensyn til retshåndhævelsen kan kun ske under overholdelse af strenge betingelser[3]. Det må navnlig kun finde sted i et begrænset tidsrum, og når det er påkrævet, passende og sker forholdsmæssigt i et demokratisk samfund.

De retshåndhævende myndigheder skal have effektive beføjelser i kampen mod terrorisme, men de må ikke være ubegrænsede eller misbruges. Der skal skabes en forholdsmæssig balance for at sikre, at vi ikke undergraver den type samfund, vi gerne vil beskytte. Denne balance er især påkrævet, når udbyderne af kommunikationstjenester tvinges til at lagre data, de ikke selv har brug for. På denne måde kunne man til sidst nå frem til en hidtil uset, vedvarende, udbredt overvågning af alle borgeres forskellige former for kommunikation og bevægelser i deres dagligdag. En enorm mængde oplysninger ville blive lagret, som kun vil være egentlig nyttige for efterforskning i et begrænset antal tilfælde.

Man bør desuden være opmærksom på, at en så omfattende forpligtelse til lagring af data vil påvirke nogle former for kommunikation, som rejser ømtålelige spørgsmål i forbindelse med visse kategorier af forretningshemmeligheder og/eller efterforskningsmæssig fortrolighed eller visse aktiviteter, der foregår i bestemte institutioner, som er specifikt beskyttet af loven.

Af denne årsag har både artikel 29-gruppen og konferencen af europæiske databeskyttelsesmyndigheder nu i nogle år haft en fast og klar holdning. Ved adskillige lejligheder siden 1997 har gruppen[4] og den europæiske konference[5] stillet spørgsmålstegn ved nødvendigheden af generelle bestemmelser om lagring af data.

---

[3] Se især artikel 15, stk. 1, i direktiv 2002/58/EF.

[4] Se følgende (*alle dokumenter kan findes på http://europa.eu.int/comm/internal_market/privacy*):

-**Udtalelse 9/2004** om et udkast til rammeafgørelse [..] (Rådets dokument nr. 8958/04 of 28. april 2004). Et resumé af nedenstående udtalelser kan findes i bilaget til denne udtalelse
-**Udtalelse 1/2003** om lagring af trafikdata til debiteringsformål
-**Udtalelse 5/2002** om de europæiske databeskyttelsesmyndigheders erklæring på den internationale konference i Cardiff (9.-11. september 2002) om obligatorisk og systematisk lagring af teletrafikdata
-**Udtalelse 10/2001** om behovet for en afbalanceret fremgangsmåde i kampen mod terrorisme
-**Udtalelse 4/2001** om Europarådets udkast til konvention om cyberkriminalitet
-**Udtalelse 7/2000** om Europa-Kommissionens forslag til Europa-Parlamentets og Rådets direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor af 12. juli 2000 KOM(2000) 385
-**Henstilling 3/99** om internet-tjenesteleverandørers opbevaring af trafikdata af hensyn til retshåndhævelsen
-**Henstilling 2/99** om beskyttelse af privatlivets fred i forbindelse med aflytning af telekommunikationer
-**Henstilling 3/97** on anonymitet på Internettet.

[5] Se de udtalelser, der blev vedtaget i Stockholm (april 2000) og Cardiff (april 2002).

II. FORELØBIG VURDERING OG GENERELLE FORUDSÆTNINGER

1. Lagrede data kan være et nyttigt redskab for efterforskere, men ovennævnte betingelser skal være tydeligt påvist og underbygget.

For det første skal målet med foranstaltningen fremgå meget klart. For det andet skal begrundelsen for obligatorisk og generel lagring af data påvises klart og dokumenteres. Det gælder også de maksimale lagringsperioder, der skal gælde. For det tredje skal det fremgå tydeligt, under hvilke betingelser de kompetente myndigheder kan få adgang til og benytte sådanne data til bekæmpelse af truslen om terrorisme.

Dokumentationen skal evalueres regelmæssigt og resultaterne heraf offentliggøres, idet der også skal tages hensyn til, at indførelse af foranstaltninger til generel overvågning af borgerne kan betyde, at man i forbindelse med terrorisme og organiseret kriminalitet vil undgå at benytte visse metoder. Det vil betyde, at man bliver nødsaget til at udvikle nye metoder til endnu strengere overvågning og dermed udløser en kaskade af mulige krænkelser af borgernes grundlæggende rettigheder, som det bliver vanskeligt at stoppe. Desuden vil det ændre karakteren af det samfund, vi søger at bevare.

Gruppen erkender, at nogle vilkår har ændret sig i vore samfund med hensyn til risikoen for terrorisme, og har fået oplyst, at visse data undertiden kan være nyttige og anvendes med god grund i forbindelse med visse efterforskninger. Endvidere bemærker gruppen, at Kommissionens initiativ i sidste ende kan føre til maksimale lagringsperioder, der er kortere end dem, man tidligere benyttede, og som gruppen udtalte sig negativt om – senest i udtalelse nr. 9/2004 af 9. november 2004, WP 99.

Imidlertid synes begrundelserne for lagring af data ikke at være baseret på krystalklare beviser, selv om de siges at være baseret på anmodninger fra de kompetente myndigheder i medlemsstaterne. Derfor ser de foreslåede vilkår endnu ikke overbevisende ud.

Der findes andre nyttige foranstaltninger i forbindelse med efterforskninger, der i mindre grad krænker borgernes grundlæggende rettigheder, f.eks. "quick freeze-proceduren", hvor hverken kommunikationsudbyderne eller internetudbyderne tvinges til at lagre trafikdata. I begrundede tilfælde henvender de retshåndhævende myndigheder sig til selskaberne og anmoder om lagring af visse data. Når disse data er lagret, får myndighederne nogle uger til at indsamle beviser for at få en dommerkendelse. Derefter kan de på grundlag af denne kendelse få adgang til dataene.

Under alle omstændigheder skal der gælde klare regler for en generel lagringsperiode. Den skal være så kort som muligt og ligge tættest muligt på lagringsperioden for det oprindelige formål med tjenesteudbyderens lagring af dataene.

2. I forbindelse med den harmonisering af medlemsstaternes lovgivning, som Kommissionen nu foreslår, bør det stå klart, at bestemmelsen om en bindende lagringsperiode på EU-plan er baseret på en proportionalitetsvurdering på EU-plan, hvor man blandt andet tog hensyn til, at organiseret kriminalitet foregår på tværs af grænserne, og til samtlige medlemsstaters sikkerhedskrav.

Derefter skal det gøres klart, at den datalagringsperiode, der henvises til i direktivet, skal betragtes som den maksimale harmoniserede tærskelværdi for alle medlemsstaterne.

Der skal derfor ikke herske tvivl om, at medlemsstaterne ikke skal sørge for længere lagringsperioder end i direktivet – selv om de frit kan fastsætte kortere lagringsperioder. Det skal også erindres, at dataene skal slettes, når perioderne er udløbet. På den baggrund er den nuværende formulering af artikel 11 i direktivforslaget ikke tilfredsstillende.

Artikel 29-gruppen glæder sig over, at forslaget indeholder en artikel om evaluering (artikel 12), som skal foretages mindst hvert andet år.

Denne evaluering skal omfatte nødvendigheden af de trafikdata, som de retshåndhævende myndigheder bruger i specifikke og klart definerede sager, og skal inddrage databeskyttelsesmyndighederne. Resultatet af disse evalueringer skal offentliggøres.

Det skal dog påpeges, at denne evaluering ikke skal foretages for et ikke nærmere bestemt tidsrum, eftersom forslaget er baseret på en konkret vurdering af de antagelser og forudsætninger, det omhandler. De påtænkte foranstaltninger til datalagring skal derfor være tidsbegrænset i overensstemmelse med begrebet "solnedgangslovgivning". Gruppen finder en periode på tre år passende. Når denne periode er udløbet, ophører virkningen af de nationale gennemførelsesforanstaltninger om datalagring – uden at dette dog berører muligheden for at indlede den analyse, der er påkrævet for at udarbejde en ny afgørelse fra Rådet og Europa-Parlamentet om et nyt direktiv, hvilket også kan ske inden den treårige periodes udløb.

Hvad angår proportionalitetsprincippet hilser artikel 29-gruppen det også velkomment, at man vil begrænse de datasæt, der skal lagres om internetbrug. Endvidere er det at foretrække at have et maksimalt datasæt til lagring frem for en minimumsliste. Generelt skal de data, der skal lagres, begrænses til dem, der er indsamlet af udbyderne af tekniske årsager og med henblik på fakturering.

Det er afgørende at tage stilling til adgang til dataene og anvendelsesformål for at sikre, at alle generelle foranstaltninger til lagring af data ledsages af de strengeste sikkerhedsforanstaltninger, og at de generelle foranstaltninger revideres.

3. De sikkerhedsforanstaltninger, der er til rådighed inden for de nugældende bestemmelser om databeskyttelse under første søjle (direktiv 95/46/EF og 2002/58/EF), bør specificeres yderligere, eftersom det særlige formål med lagringen af data er at lette retshåndhævelsen. Specifikke sikkerhedsforanstaltninger er afgørende for at sikre, at den beskyttelse, direktiv 2002/58/EF giver, især retten til fortrolighed i forbindelse med brug af offentligt tilgængelige elektroniske kommunikationstjenester, ikke undergraves væsentligt.

Endvidere er gruppen af den opfattelse, at der bør være passende sikkerhedsforanstaltninger for databehandlingstransaktioner i sektorer, som i øjeblikket falder uden for disse direktivers anvendelsesområde.

Derfor mener gruppen blandt andet, at selve direktivforslaget bør indeholde sådanne sikkerhedsforanstaltninger, eller at de bør evalueres og vedtages sammen med andre passende retsmidler. Mere specifikt finder gruppen, at rammeafgørelsen om beskyttelse af persondata, der

behandles i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, også skal vurderes omhyggeligt i denne forbindelse.

Endelig mener gruppen på baggrund af virkningen for de berørte borgeres grundlæggende rettigheder og frihedsrettigheder, at de foranstaltninger, der kan blive indført, skal offentliggøres bredt.

III. ANDRE SPECIFIKKE SIKKERHEDSFORANSTALTNINGER

Endvidere finder gruppen, at i hvert fald følgende spørgsmål bør tages op:

1. FORMÅL

Dataene skal kun lagres med det specifikke formål at bekæmpe terrorisme og organiseret kriminalitet frem for det ubestemte "grov kriminalitet". Dette begrænsede formål bør der også henvises til i direktivforslaget.

2. MODTAGERE

Det skal fremgå af direktivet, at dataene kun kan stilles til rådighed for særligt udpegede retshåndhævelsesmyndigheder, når det er nødvendigt af hensyn til efterforskning, afsløring, retsforfølgning og/eller forebyggelse af terrorisme. En liste over sådanne udpegede retshåndhævelsesmyndigheder skal være offentligt tilgængelig.

3. DATAMINING

Forebyggelse af terrorisme skal ikke omfatte udbredt datamining med udgangspunkt i de oplysninger, der henvises til i direktivet, med hensyn til rejse- og kommunikationsmønstre for personer, som de retshåndhævende myndigheder ikke nærer mistanke til. Adgangen skal begrænses til de data, der er nødvendige for den specifikke efterforskning.

4. YDERLIGERE BEHANDLING

Enhver yderligere behandling af lagrede data foretaget af de retshåndhævende myndigheder i forbindelse med andre lignende procedurer bør udelukkes eller begrænses mest muligt ved hjælp af specifikke sikkerhedsforanstaltninger, og det skal forhindres, at andre end offentlige organer får adgang til dataene. Reglerne i tidligere EU-retsakter om sektoren for elektronisk kommunikation må ikke anvendes på en måde, der er i strid med dette princip.

5. ADGANGSREGISTRERING

Enhver udlæsning af data skal registreres. Optegnelserne må kun være tilgængelige efter anmodning for den myndighed og/eller det organ, der er nævnt i punkt 6 nedenfor, samt for databeskyttelsesmyndighederne i forbindelse med kontrol og skal slettes et år efter forelæggelsen.

6. DOMSTOLSKONTROL/UAFHÆNGIG KONTROL

Adgang til data bør i princippet gives i hvert enkelt tilfælde af en retsmyndighed, idet der dog i nogle lande kan være en specifik mulighed for adgang i medfør af en lov, og der bør være en uafhængig kontrolinstans. Når det er muligt, skal tilladelserne specificere de særlige data, der er behov for i de pågældende sager.

7. ADRESSATER

Det skal fremgå tydeligt af direktivet, hvilke udbydere af offentlige kommunikationstjenester der er omfattet af forpligtelserne. I forbindelse med internetdata er der behov for en begrænsning for internetudbyderen og individuel kommunikation (e-mailtjenester, taletelefoni via IP).

8. IDENTIFIKATION

Det er vigtigt at afklare også i dette direktiv, at der ikke er nogen forpligtelse til identifikation i tilfælde, hvor identifikation ikke er nødvendig af hensyn til faktureringen eller andre forhold med henblik på at opfylde kontrakten.

9. HENSYNET TIL DEN OFFENTLIGE RO OG ORDEN

Udbydere af offentlige elektroniske kommunikationstjenester eller –net skal ikke have tilladelse til at behandle data, der kun er lagret af hensynet til den offentlige ro og orden, til egne formål.

10. SYSTEMADSKILLELSE

Systemerne til lagring af data af hensyn til den offentlige ro og orden skal være logisk adskilt fra systemer, som udbyderne bruger forretningsmæssigt, og beskyttet af strengere sikkerhedsforanstaltninger (f.eks. gennem kryptering) for at forhindre uautoriseret adgang og brug.

11. SIKKERHEDSFORANSTALTNINGER

Fællesskabsforanstaltningerne skal omfatte minimumsstandarder for de tekniske og organisatoriske sikkerhedsforanstaltninger, som udbyderne skal træffe, med angivelse af de generelle krav til sikkerhedsforanstaltninger i henhold til direktiv 2002/58/EF.

12. TREDJEMAND

Det skal fremgå af fællesskabsforanstaltningerne, at enhver tredjemands adgang til de lagrede data er ulovlig.

13. DEFINITIONER

Datakategorier skal defineres klart, og der skal fastsættes en begrænsning af trafikdata.

14. LISTER OVER DATA OG MEKANISMER TIL DATAREVISION

Det er nødvendigt, at direktivet direkte specificerer, hvilke personlige data der skal lagres. Det er vigtigt for at få et nøjagtigt udtryk for virkningen for de berørte borgeres grundlæggende rettigheder og frihedsrettigheder under hensyn til risiciene for deres privatliv og spørgsmål i forbindelse med at sikre nøjagtigheden og aktualiteten af de lagrede data. Alle forslag om ændringer af listen over datatyper, der skal lagres, skal afprøves for at fastslå, om de er strengt nødvendige. På baggrund af virkningerne af disse foranstaltninger for de grundlæggende rettigheder og frihedsrettigheder foretages revisionen af listen udelukkende med Europa-Parlamentets godkendelse og under inddragelse af databeskyttelsesmyndighederne. Man bør desuden inddrage repræsentanter for forbrugere og brugere, andre relevante ikke-statslige organer og europæiske sammenslutninger i den elektroniske kommunikationsindustri. På denne baggrund synes det ikke at være passende at revidere listen i henhold til komitologiproceduren, som man forestiller sig i direktivet.

15. INGEN DATA OM INDHOLD

Da forslaget tager sigte på at udelukke indholdet af kommunikationen, skal der indføres specifikke garantier om en skarp, effektiv sondring mellem indholds- og trafikdata – både hvad

angår internettet (dvs. kun data om log-in/log-off, og andre former for oplysninger som logs over mailservere, web caches og IP flow) og telefoni (telefonmøder, fax, sms, taletelefoni).

16. MISLYKKEDE KOMMUNIKATIONSFORSØG

De forskellige kategorier af trafikdata om mislykkede kommunikationsforsøg skal ikke medtages, da der ikke foreligger en tilbundsgående vurdering af nytten heraf på grundlag af ovennævnte principper.

17. LOKALISERINGSDATA

Lagring af lokaliseringsdata må kun omfatte apparatets lokaliseringskode ved indledningen af kommunikationen.

18. EFFEKTIVT TILSYN

Der skal foretages effektiv kontrol med retsmyndighedernes oprindelige og eventuelle senere tilladelige anvendelse af data (herunder mangfoldiggørelse) i forbindelse med en strafferetlig procedure, og med databeskyttelse i forbindelse med databeskyttelsesmyndighedernes brug af data, uanset om der er tale om en strafferetlig procedure.

19. ÅBENHED

Direktivet bør indeholde et krav om, at alle borgere skal underrettes behørigt om enhver form for behandling af data efter gennemførelsen af dets bestemmelser.

20. OMKOSTNINGER

Artikel 29-gruppen bemærker, at medlemsstaterne skal dække supplerende omkostninger for udbydere af offentlige elektroniske kommunikationstjenester eller -net. Gruppen vil gerne understrege vigtigheden af dette spørgsmål alene med hensyn til de forhold, der vedrører databeskyttelse direkte. Foranstaltninger i forbindelse med lagring af data bør desuden omfatte refusion af investeringer i tilpasning af kommunikationssystemer og af udgifter i forbindelse med afgivelse af oplysninger til de retshåndhævende myndigheder og sikkerhedsforanstaltninger. Det er nødvendigt at anlægge en bred synsvinkel for at forhindre eventuelle negative virkninger både med hensyn til databeskyttelse og de økonomiske forhold for borgere, som kan blive pålagt nogle af udbydernes omkostninger. I denne forbindelse kunne man desuden overveje, om en udbyders ret til refusion af omkostninger skal gøres afhængig af, at vedkommende opfylder minimumsstandarderne, og om den skal vurderes i hvert enkelt tilfælde.

Gruppen er overbevist om, at der vil blive taget behørigt hensyn til betragtningerne i dens udtalelse, og minder om, at alle de sikkerhedsforanstaltninger, der er nævnt ovenfor, skal gennemføres inden forpligtelserne til lagring af data træder i kraft.

Udfærdiget i Bruxelles, den 21. oktober 2005

På gruppens vegne

Peter Schaar
Formand

ARTICLE 29 Data Protection Working Party

1868/05/EN
WP 113

Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)

Adopted on 21st October 2005

EXECUTIVE SUMMARY

The European Commission's Proposal for a Directive on the retention of data is confronting us with a historical decision.

Traffic data retention interferes with the inviolable, fundamental right to confidential communications.

Any restriction on this fundamental right must be based on a pressing need, should only be allowed in exceptional cases and be the subject of adequate safeguards.

Providers of publicly available communication services would be forced unprecedentedly to store billions of data relating to the communications of any and all citizens for investigational purposes.

Terrorism presents our society with a real and pressing challenge. Governments must respond to this challenge in a way that effectively meets their citizens need to live in peace and security while not undermining their individual human rights – including the right to data privacy- which are a cornerstone of our democratic society.

The European Commission's initiative might ultimately result in setting out maximum retention periods that are shorter than those envisaged in other recent proposals.

The Working Party questions whether the justification for an obligatory and general data retention coming from the competent authorities in Member States is grounded on crystal-clear evidence. The Working Party also doubts whether the proposed data retention periods in the draft Directive are convincing.

As just mentioned above, the justification for any compulsory and general data retention must be clearly demonstrated and backed up with evidence. This also applies to the maximum periods that should apply in such a case. In any case, the conditions under which the competent authorities could access and use such data in order to combat the threat of terrorism should also be clearly spelled out.

The purposes of data retention should be stated clearly in the Directive by having regard to the fight against terrorism and organised crime rather than against any undetermined "serious crime".

Account should be taken that there are less privacy-intrusive approaches (e.g. the quick-freeze procedure).

The retention period of the data, if any, should be as short as possible and represent the maximum retention threshold applying to all Member States, even though they will be free to lay down shorter retention periods. The measures possibly introduced should be broadly publicized.

The evidence supporting these measures should be evaluated periodically. Based on a periodical assessment, to be performed at least every two or three years and made public, the envisaged data retention measures should be time-limited pursuant to the "sunset legislation" concept. A three-year term is considered suitable.

In any case, imposing the said data retention obligations on communication service providers without having first realised adequate, specific safeguards is not to be accepted within the existing European legal framework.

Finally, the Working Party set out twenty specific safeguards to be envisaged with particular regard to the requirements applying to recipients and further processing, the need for authorisations and controls, the measures applying to service providers also in terms of security and logical separation of the data, the determination of the data categories involved and their updating, and the need to rule out contents data.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS
WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 (1)(a) and (3) of that Directive and 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

having regard to its Rules of Procedure, and in particular Articles 12 and 14 thereof,

has adopted the following Opinion:

I. Background

Within the framework of the European initiatives to fight terrorism and organised crime, on the last 21st of September the European Commission presented a "*Proposal for a Directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC* [1]".

The issue in question is of considerable importance to all citizens.

Freedom and confidentiality of correspondence and all other forms of communication are among the pillars of modern democratic societies. Their inviolability has been set forth in several instruments, including constitutional charters, as well as being specifically safeguarded in the European Convention on Human Rights which Community law has set as its own foundations.

The proposed Directive is confronting us with a historical decision. It is aimed at introducing, for the first time, the Europe-wide obligation to retain, for investigational purposes, billions of data relating to the communications of any and all citizens. Under Community law, such data are currently not stored or else are retained only on a temporary basis by electronic communications service providers - and if so, exclusively for contractual purposes.

Traffic data retention interferes with the fundamental right to confidential communications guaranteed to the individuals by Article 8 of the European Convention on Human Rights. In a democratic society, any interference with this fundamental right can be justified if it is necessary in the interests of national security. It can ultimately result in keeping track of and charting all contacts and relationships held by individuals as well as the places in which this happens and the means used for such purposes The European Court of Human Rights has also stressed that secret surveillance poses a danger of undermining or even destroying democracy on the ground of defending it; additionally, the Court has affirmed that States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. [2]

[1] [COM (2005) 438 final], 21.9.2005, *not yet published in O.J.*

This is why any restrictions of this fundamental right must be based on a pressing need, should only be allowed in exceptional cases and be the subject of adequate safeguards. The retention of traffic data -including location data- for purposes of law enforcement should meet strict conditions, [3] in particular it must take place only for a limited period and when necessary, appropriate and proportionate in a democratic society.

The powers available to law enforcement agencies in the fight against terrorism must be effective, but they cannot be unlimited or misused. A proportionate balance must be struck to ensure that we do not undermine the kind of society we are seeking to protect. This balance is especially necessary when forcing communication service providers to store data that they themselves have no need for. In this manner, one could eventually achieve the unprecedented, continued, pervasive monitoring of all kinds of communication and movement of the totality of citizens in their daily life. A huge amount of information would be stored that is actually useful for investigational purposes in a limited number of cases.

Consideration should also be given to the circumstance that such a sweeping data retention obligation impacts on some communications that raise delicate issues in connection with certain categories of professional and/or investigational secrecy, or certain activities by particular institutions, that are protected specifically by the law.

For this reason, for some years now the view of both the Article 29 Working Party and the Conference of European Data Protection Authorities has been firm and clear. Upon several occasions since 1997, the Working Party [4] and the European Conference [5] have questioned the necessity of general data retention measures.

---

[2] Klass and others v. Germany, para. 49.

[3] See, in particular, article 15(1) of Directive 2002/58/EC.

[4] See (*all documents are available at http://europa.eu.int/comm/internal_market/privacy*):

-**Opinion 9/2004** on a draft Framework Decision [..] (Document of the Council 8958/04 of 28 April 2004). A summary of the following statements can be found in the annex to this opinion;
-**Opinion 1/2003** on the storage of traffic data for billing purposes;
-**Opinion 5/2002** on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data;
-**Opinion 10/2001** on the need for a balance approach in the fight against terrorism;
-**Opinion 4/2001** on the Council of Europe's Draft Convention on Cyber-crime;
-**Opinion 7/2000** on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385;
-**Recommendation 3/99** on the preservation of traffic data by Internet Service Providers for law enforcement purposes;
-**Recommendation 2/99** on the respect of privacy in the context of interception of telecommunications;
-**Recommendation 3/97** on Anonymity on the Internet.

[5] See the statements adopted in Stockholm (April 2000) and Cardiff (April 2002).

II. PRELIMINARY ASSESSMENT AND GENERAL PRECONDITIONS

1. Retained data may provide a useful tool for investigators, but the above mentioned conditions should be clearly demonstrated and substantiated.

Firstly, the aim of such a measure should be stated very clearly. Secondly, the justification for compulsory and general data retention must be clearly demonstrated and backed up with evidence. This also applies tot the maximum periods that should apply in such a case. Thirdly, the conditions under which the competent authorities could access and use such data in order to combat the threat of terrorism should be clearly spelled out.

That evidence should at least be evaluated periodically and the results published, taking also into account that introducing means of general surveillance of citizens might cause strategies on the side of terrorism and organized crime not to use certain means. This would result in the necessity to develop new methods of even stricter surveillance thus setting into motion a spiral of possible infringements of the fundamental rights of citizens which will be hard to stop. Furthermore, this would change the character of the society we are striving to preserve.

The Working Party acknowledges that some conditions have changed in our societies as for the risks posed by terrorist threats, and has been informed that some data may at times be helpful and justifiably used in certain investigations. Additionally, the Working Party notes that the European Commission's initiative might ultimately result into setting out maximum retention periods that are shorter than those envisaged in the past, on which the Working Party expressed itself unfavourably – lastly via Opinion no. 9/2004 adopted on 9 November 2004, WP 99.

However, the circumstances justifying data retention, even though they are said to be based on the requests coming from the competent authorities in Member States, do not appear to be grounded on crystal-clear evidence. Accordingly, the proposed terms do not appear convincing as yet.

There exist other useful measures to be taken into account for investigational purposes, which infringe to a lesser extent upon the basic right positions of the citizens, e.g. the "quick freeze-procedure" where neither the communication providers nor the Internet service providers are obliged to store traffic data. For instance, in well-founded cases, the law enforcement agencies consult the companies and request the storage of certain data. After those data have been stored, the agencies are given some weeks to collect evidence in order to obtain a judicial order. Then, based on this order, they can access the data.

In any event, a general retention period must be clearly regulated. Such retention period should be as short as possible and should be as close as possible to the retention period for the original purposes for which communication service providers recorded those data.

2. The harmonisation of Member States' legislation currently proposed by the Commission should clarify that the provision for a binding data retention period at European level is based on a proportionality assessment carried out at European level by taking also account of the transnational character of organised crime as well as of the maximum security requirements of all Member States.

Then, it will have to be clarified that the data retention period referred to in the Directive is to be regarded as the maximum harmonised threshold applying to all Member States.

Therefore, it should be made clear that Member States will not have to provide for longer data retention periods than the Directive – even though they will be free to lay down shorter retention periods. It should also be recalled that the data are to be erased at the end of the said periods. Given this context, the current wording of Article 11 in the draft Directive is not satisfactory.

The Article 29 Working Party welcomes that the proposal contains an article on an evaluation (Article 12), to be carried out periodically at least every two years.

This evaluation should include the necessity of the traffic data used by law enforcement authorities in specific and well identified cases, and should involve the data protection authorities. The result of these evaluations should be published.

However, it should be pointed out that the said evaluation should not be performed with regard to an undetermined amount of time, given that the proposal is based on the concrete assessment of the assumptions and prerequisites it refers to. Therefore, the envisaged data retention measures should be time-limited pursuant to the "sunset legislation" concept. A three-year term is considered suitable by the Working Party. Upon expiry of this term, the national implementing measures mandating data retention should cease to be effective - without prejudice to the possibility of starting the analysis required to prepare a new decision by the Council and the European Parliament endorsing a new Directive also prior to the expiry of the three-year term.

With regard to the principle of proportionality, the Article 29 Working Party also welcomes the limitation of the set of data to be retained with regard to the use of Internet. Moreover, a maximum set of data to be retained has to be preferred over a minimum list. Generally, the data to be retained should be restricted to those collected by the providers for technical and billing purposes.

It is essential to determine the access to data and purposes of use, to ensure that any general data retention measures are accompanied by the strongest safeguards, and to submit such measures to audit.

3. The safeguards available within the existing legal framework on data protection in the first pillar (Directives 95/46/EC and 2002/58/EC) should be further specified for the particular law enforcement context of traffic data retention. Specified safeguards are vital to ensure that the protection offered by Directive 2002/58/EC, in particular to the right of the confidentiality of the use of publicly available electronic communication services, is not substantially undermined.

Additionally, the Working Party is of the opinion that adequate safeguards should be in place regarding data processing operations in sectors that at present fall outside the scope of these directives.

This is why the Working Party holds the view, inter alia, that the draft Directive should itself provide for these safeguards, or otherwise be evaluated and adopted jointly with other adequate legal instruments. In particular, the Working Party considers that the "Framework Decision on

the protection of personal data processed in the framework of police and judicial cooperation in criminal matters" shall be carefully assessed also within this context.

Finally, given the impact on fundamental rights and freedoms of the citizens concerned, the Working Party believes that the measures possibly introduced should be broadly publicized.

III. OTHER SPECIFIC SAFEGUARDS

In addition, the Working Party considers that the following issues should at least be addressed:

1. PURPOSES

The data should only be retained for specific purposes of fighting terrorism and organised crime, rather than with regard to any other undetermined "serious crime". This limited purpose should be also referred to in the title of the proposed Directive.

2. RECIPIENTS

The Directive should provide that the data be only available to specifically designated law enforcement authorities where necessary for the investigation, detection, prosecution and/or prevention of terrorism. A list of such designated law enforcement authorities should be publicly available.

3. DATA MINING

Prevention of terrorism should not include large-scale data-mining based on the information referred to in the Directive in respect of the travel and communication patterns of people unsuspected by the law enforcement authorities. Access must be restricted to those data that are necessary in the context of specific investigation.

4. FURTHER PROCESSING

Any further processing of retained data by law enforcement authorities for other related proceedings should be ruled out or limited stringently on the basis of specific safeguards, and any access to the data by other government bodies should be prevented. The rules set out in previous European legal instruments concerning the electronic communications sector may not be applied in a manner that is inconsistent with this principle.

5. ACCESS LOGS

Any retrieval of the data should be recorded. The records should only be available, upon request, to the authority and/or body mentioned below in point 6 as well as to data protection authorities in case of control, and have to be deleted one year after being produced.

6. JUDICIAL/INDEPENDENT SCRUTINY

Access to data should, in principle, be duly authorised on a case by case basis by a judicial authority without prejudice to countries where a specific possibility of access is authorised by law, subject to independent oversight. Where appropriate, the authorisations should specify the particular data required for the specific cases at hand.

7. ADDRESSEES

The Directive should clearly define which providers of publicly available communication services are concerned by the obligations. In the case of the Internet, a limitation on access provider and one-to-one communication (e-mail services, voice over IP) is necessary.

8. IDENTIFICATION

It is important to clarify also in this Directive that there is no obligation for identification in cases where the identification is not necessary for billing purposes or other purposes to fulfil the contract.

9. PUBLIC ORDER PURPOSES

Providers of public electronic communication services or networks should not be allowed to process data retained solely for public order purposes for their own purposes.

10. SYSTEM SEPARATION

In particular, the systems for storage of data for public order purposes should be logically separated from systems that are used for the business purposes of providers and protected by more stringent security measures (for instance by means of encryption) in order to prevent unauthorized access and use.

11. SECURITY MEASURES

The Community measures should provide for minimum standards for technical and organisational security measures to be taken by the providers, specifying the general requirements regarding security measures established in Directive 2002/58/EC.

12. THIRD PARTIES

The Community measures should specify that access to retained data by any other third parties is illegitimate.

13. DEFINITIONS

There should be a clear definition of the data categories and a limitation on traffic data.

14. LIST OF DATA AND MECHANISMS FOR ITS REVISION

It is necessary for the Directive to directly specify the list of personal data to be retained. This is important in order to accurately gauge the impact on fundamental rights and freedoms of the citizens concerned, by having regard to the risks for their personal sphere and taking also account of the issues related to ensuring accuracy and updating of the retained data. Any proposals for changes to the list of the types of data to be retained should be subjected to a strict necessity test. In the light of the impact of these measures on fundamental rights and freedoms, the revision of the said list should be carried out only with the approval of the European Parliament and by involving data protection authorities. The participation of representatives from consumer and user associations, other relevant non-governmental bodies, and the European associations of the electronic communications industry should also be envisaged. In this perspective, it does not appear to be appropriate to carry out the revision of the said list merely according to the comitology procedure as envisaged in the Directive.

15. NO CONTENTS DATA

Since the scope of the proposal is meant to exclude contents of communications, specific guarantees should be introduced in order to ensure a stringent, effective distinction between contents and traffic data – both for the Internet (i.e., only log-in/log-off data, or else any information, including mail server logs, web cache logs and IP flow logs) and for telephony (conference calls, fax, sms, voice).

16. UNSUCCESSFUL COMMUNICATION ATTEMPTS

The different categories of traffic data related to unsuccessful communication attempts should not be included, failing an in-depth adequacy assessment in the light of the principles mentioned above.

17. LOCATION DATA

Storing location data should not go beyond the cellID at the start of a communication.

18. EFFECTIVE SUPERVISION

There should be effective controls on the original and on any further compatible use (including duplication), by judicial authorities within and for the purposes of a criminal procedure and, concerning data protection regardless of the existence of a judicial proceeding, by data protection authorities.

19. PUBLICITY

The Directive should envisage the obligation to adequately inform all citizens with regard to any and all processing operations to be possibly performed further to the implementation of its measures.

20. COSTS

The Article 29 Working Party notes that additional costs upon providers of public electronic communication services or networks are to be compensated by Member States. The Working Party would like to stress the importance of this issue exclusively with regard to the features that are directly related to data protection. Data retention measures should also involve both reimbursement for investments in the adaptation of the communication systems, for the disclosure of data to law enforcement authorities and about security measures. A comprehensive view is required in order to prevent any negative effects from being produced both on the data protection level and on the economic sphere of citizens, who might be charged some of the costs incurred by providers. In this context, it might also be considered whether a provider's entitlement to reimbursement for costs should be subject to fulfilment of the minimum standards and should take place on a case-by-case basis.

The Working Party is confident that the considerations made in its Opinion will be taken into due account, and recalls that all the safeguards mentioned above should be in place prior to putting into practice data retention obligations.

Done at Brussels, on 21st of October 2005

For the Working Party

The Chairman

Peter Schaar

I

(Information)

OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final)

(2005/C 298/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data [1] and on the free movement of such data and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [3], and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 23 September 2005 from the Commission;

HAS ADOPTED THE FOLLOWING OPINION:

I Introduction

1. The EDPS welcomes the fact that he is consulted on the basis of Article 28(2) of Regulation (EC) No 45/2001. However, in view of the mandatory character of Article 28(2) of Regulation (EC) No 45/2001, the present opinion should be mentioned in the preamble of the directive.

2. The EDPS recognises the importance for law enforcement agencies of the Member States of having all the necessary legal instruments at their disposal, in particular in

[1] OJ L 281, 23.11.1995, p. 31.

[2] OJ L 201, 31.7.2002, p. 37.

[3] OJ L 8, 21.1.2001, p. 1.

the combat of terrorism and other serious crime. An adequate availability of certain traffic and location data of public electronic services can be a crucial instrument for those law enforcement agencies and can contribute to the physical security of persons. In addition it should be noted that this does not automatically imply the necessity of the new instruments as foreseen in the present proposal.

3. It is equally evident that the proposal has a considerable impact on the protection of personal data. If one considers the proposal solely from the perspective of data protection, traffic and location data should not be retained at all for the purpose of law enforcement. It is for reasons of data protection that Directive 2002/58/EC establishes as a principle of law that traffic data must be erased as soon as storage is no longer needed for purposes related to the communication itself (including billing purposes). Exemptions to this principle of law are subject to strict conditions.

4. In this opinion, the EDPS shall highlight the impact of the proposal on the protection of personal data. The EDPS shall furthermore take into account that, not withstanding the importance of the proposal for law enforcement, it may not result in people being deprived of their fundamental right to have their privacy protected.

5. This opinion of the EDPS must be seen in the light of these considerations. The EDPS envisages a balanced approach, in which the necessity and the proportionality of the interference with data protection play a central role.

6. As to the proposal itself, this must be seen as a reaction to the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism ('the draft Framework Decision'), that was rejected by the European Parliament (in the consultation procedure).

7. The EDPS has not been consulted on the draft Framework Decision, nor has he given an opinion on his own initiative. The EDPS does not intend to give as yet an opinion on the draft Framework Decision, but will in the present opinion refer to this draft decision, where he deems this to be useful.

II General observations

The impact of the proposal on the protection of personal data

8. It is essential to the EDPS that the proposal respects the fundamental rights. A legislative measure which would harm the protection guaranteed by Community law and more in particular by the case-law of the Court of Justice and the European Court of Human Rights is not only unacceptable, but also illegal. The circumstances in society may have changed due to terrorist attacks, but this may not have as an effect that high standards of protection in the state of law are compromised. Protection is given by law irrespective of the actual needs of law enforcement. Moreover, the case-law itself allows for exceptions, if necessary in a democratic society.

9. The proposal has a direct impact on the protection given by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the 'ECHR'). According to the case-law of the European Court of Human Rights:

— The storing of information about an individual was considered to be an interference with private life, even though it contained no sensitive data (Amann ([1])).

— The same applies to the practice of 'metering' of telephone calls, which involves the use of a device that registers automatically the numbers dialled on a telephone and the time and the duration of each call (Malone ([2])).

— Justifications for interference should outweigh the detrimental effect that the very existence of the legislative provisions in question could have on the subjects (Dudgeon ([3])).

10. Article 6(2) of the EU-Treaty provides that the Union shall respect fundamental rights, as guaranteed by the ECHR. In the preceding paragraph it has been shown that, under the case-law of the European Court of Human Rights, the obligation to retain data falls within the scope of Article 8 ECHR and that a pressing justification is needed that respects

([1]) Judgment of the ECHR of 16 February 2000, Amann, 2000-II, Appl. 27798/95.

([2]) Judgment of the ECHR of 2 August 1984, Malone, A82, Appl. 8691/79.

([3]) Judgment of the ECHR of 22 October 1981, Dudgeon, A45, Appl. 7525.

the criterion of the Dudgeon-judgement. The necessity and the proportionality of the obligation to retain data — in its full extent — have to be demonstrated.

11. In addition, the proposal has a huge impact on principles of data protection recognised by Community law:

— The data have to be retained over a period far longer than the periods that are usual for retention by providers of publicly available electronic communications services or by a public communications network (both services are hereafter referred to as 'providers').

— Under Directive 2002/58/EC, more in particular its Article 6, data may only be collected and stored for reasons directly related to the communication itself, including billing purposes ([1]). Afterwards, data must be erased (subject to exceptions). Under the present proposal, retention for the purpose of enforcement of criminal law is mandatory. The point of departure is thus contrary.

— Directive 2002/58/EC ensures security and confidentiality. This proposal may not lead to loopholes in that field; strict safeguards are required and the purpose limitation should be clarified.

— The introduction of the obligation to retain data, as foreseen by the proposal, leads to substantial databases and has particular risks for the data subject. One could think of the commercial use of the data, as well as of the use of the data for 'fishing operations' and/or data mining by law enforcement authorities or national security services.

12. Finally, the protection of private life, as well as the protection of personal data have both been recognised in the Charter on Fundamental Rights, as has been mentioned in the Explanatory Memorandum.

13. The impact of the proposal on the protection of personal data needs a thorough analysis. In this analysis, the EDPS will take the foregoing elements into account and he will conclude that more safeguards are needed. A simple reference to the existing legal framework on data protection (in particular, the directives 95/46/EC and 2002/58/EC) is not sufficient.

The necessity of retention of traffic and location data

14. The EDPS recalls the conclusion from 9 November 2004 of the Article 29 Data Protection Working Party on the draft Framework Decision. The Working Party stated that the mandatory retention of traffic data, under the conditions provided for in the draft Framework Decision, is not acceptable. This conclusion was *inter alia* based on the failure to provide any evidence as to the need of the retention for public order purposes, due to the fact that analysis showed that the most significant amount of traffic data demanded by law enforcement was not older than six months.

15. According to the EDPS, the considerations of the Article 29 Data Protection Working Party mentioned above should be the point of departure for the appraisal of the present proposal. However, the result of these considerations can not simply be transposed to the present proposal. One has to take into account that circumstances can change. According to the EDPS, the following developments could be relevant to the appraisal.

16. In the first place, some figures have been produced to demonstrate that in practice traffic data up to one year old are demanded by law enforcement. The Commission as well as the Presidency of the Council attach importance to a study by the police of the United Kingdom ([2]) that shows that although 85 % of the traffic data required by the police was less than six months old, the data between six months and a year were used in complex investigations into more serious crimes. Some examples of cases were presented as well. The retention period in the proposal — one year for telephone data — reflects these practices of law enforcement.

17. The EDPS is not convinced that these figures represent the evidence of the necessity of the retention of traffic data up to one year. The fact that in some cases the availability of traffic and/or location data helped solving a crime does not automatically mean that those data are needed (in general) as a tool for law enforcement. However, the figures can not be ignored. They represent at least a serious attempt to demonstrate the necessity of the retention. Moreover, the figures clearly indicate that a retention period for over one year is not required from the perspective of the current practices of law enforcement.

18. In the second place, the existing possibilities for the providers under Directive 2002/58/EC to retain traffic data for billing purposes are not always used, since in a growing number of cases data retention for billing purposes does not take place at all (prepaid cards for mobile communications,

([1]) See also point 3 of this opinion.

([2]) Liberty and security, striking the right balance. Paper by the UK Presidency of the European Union of 7 September 2005.

flat rate-subscriptions, etc.). In those cases — that in practice have become more frequent — traffic and location data will not be stored at all but erased immediately after the communication. The same goes for unsuccessful calls. This can have an impact on the effectiveness of law enforcement.

19. Moreover, this development in telecommunications services can lead to disturbances in the functioning of the internal market, *inter alia* due to the (imminent) adoption of legislative measures in Member States under Article 15 of Directive 2002/58/EC. For example, the Italian government recently published a decree that obliges providers to store telephone data for four years. This obligation will lead to considerable costs in certain Member States, such as Italy.

20. In the third place, the working methods of law enforcement authorities have developed as well: proactive investigations and the use of technical support have become more important. These developments require that the authorities dispose of adequate and precisely formulated tools to enable them to do their work with due respect to the principles of data protection. One of the tools the authorities in the Member States usually dispose of is data preservation, or, the freezing of communications data on request in a concrete investigation. It has been stated that this tool, that in itself has less impact on those principles than the tool that now is proposed (data retention), might not always be enough, in particular not to track persons involved in terrorism or other serious crime who were previously not suspected of any criminal activity. However, more evidence is needed to determine if this really is the case.

21. In the fourth place, the concerns about terrorist attacks have grown. The EDPS shares the view as expressed in the context of the proposals on data retention, that physical security is, in itself, of overriding importance. Society needs to be protected. For this reason governments are obliged, in case of attacks on society, to demonstrate that they give serious consideration to this need for protection and to investigate if they have to react by introducing new legislative measures. It goes without saying that the EDPS fully endorses the task of governments — on the national as well as on the European level — to protect society and to demonstrate that they do all that is needed to offer protection, including the adoption of new, legitimate and effective measures as a result of their investigations.

22. The EDPS recognises the changes of circumstances, but is as yet not convinced of the necessity of the retention of traffic and location data for law enforcement purposes, as established in the proposal. He emphasises the importance of the principle of law established by Directive 2002/58/EC that traffic data must be erased as soon as storage is no longer needed for purposes that are not related to the communication itself. Furthermore, the figures provided do not prove that the existing legal framework does not offer the instruments that are needed to protect physical security, nor that the Member States fully apply their competences under European law to cooperate as been granted to them within the existing legal framework (but without the results that are needed) .

23. However, if the European Parliament and the Council — after a careful balancing of the interests at stake — draw the conclusion that the necessity of the retention of traffic and location data is sufficiently demonstrated, the EDPS takes the view that the retention can only be justified under Community law in so far as the principle of proportionality is respected and adequate safeguards are provided, in accordance with this opinion.

The proportionality

24. The proportionality of the proposed new legislative measure itself depends on the substance of the provisions it comprises: does it comprise the adequate and proportionate response to the needs of society?

25. The first consideration touches upon the adequacy of the proposal: can one expect that the proposal increases the physical security of the inhabitants of the European Union? One reason to doubt the adequacy, often mentioned in the public debate, is that traffic data and location data are not always linked to a specified individual, so knowledge about a telephone number (or an IP-number) does not necessarily reveal the identity of an individual. Another — and even more serious — reason for doubt is whether or not the existence of gigantic data bases enables law enforcement to easily find what they need in a specific case.

26. The EDPS takes the view that retention of traffic and location data alone is in itself not an adequate or effective response. Additional measures are needed, so as to ensure that the authorities have a targeted and quick access to the data needed in a specific case. The retention of data is only adequate and effective in so far as effective search engines exist.

27. The second consideration touches upon the proportionate nature of the response. To be proportionate, the proposal should:

— limit the retention periods. The periods must reflect the demonstrated needs of law enforcement,

— limit the number of data to be stored. This number must reflect the demonstrated needs of law enforcement and it must be ensured that access to content data is not possible,

— contain adequate safety measures, so as to limit the access and further use, guarantee the security of the data and ensure that the data subjects themselves can exercise their rights.

28. The EDPS emphasises the importance of these strict limitations, with adequate safeguards in view of a limited access. He takes the view that in the perspective of the importance of the three elements mentioned in the foregoing point, the Member States may — as regards these three elements — not take additional national measures that prejudice the proportionality. This need for harmonisation will be elaborated under IV.

Adequate safety measures

29. The effect of the proposal will be that the providers will dispose of databases in which a significant amount of traffic and location data will be stored.

30. In the first place, the proposal will have to make sure that the access to and the further use of these data will be limited, only under specified circumstances and for a limited number of specified purposes.

31. In the second place, the databases will have to be adequately protected (data security). To this effect, it must be ensured that at the end of the retention periods, the data are efficiently erased. There should be no 'dumping of data' or exploitation of data. In short, this requires a high data security and adequate technical and organisational safety-measures.

32. A high data security is even more important since the mere existence of data might lead to demands for access and use, by at least three groups of stakeholders:

— the providers themselves. They might be tempted to use the data for their own commercial goals. Guarantees are necessary, preventing the copying of these files,

— authorities responsible for law enforcement: the proposal offers them a right to access, but only in specific cases and according to national legislation (Article 3(2) of the proposal). There should be no access for data mining purposes or 'fishing operations'. The exchange of data with authorities in other Member States should be clearly regulated,

— intelligence services (with responsibility for national security).

33. As to the access by intelligence services, the EDPS observes that, under Article 33 TEU and Article 64 EC interventions within the third pillar and the first pillar shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security. According to the EDPS, these provisions have as an effect that the European Union lacks the competence to control the access of security or intelligence services to the data retained by the providers. In other words, neither the access of these services to traffic and location data of the providers, nor the further use of the information acquired by these services is affected by the law of the European Union. This is an element that has to be taken into account in the appraisal of the proposal. It is the Member States that should take the necessary measures to regulate the access by intelligence services.

34. In the third place, the effects described in the previous paragraphs have potential implications for the data subject. Additional safeguards are needed so as to make sure that he can simply and quickly exercise his rights as a data subject. The EDPS points out the need of an effective control on the access and further use, preferably by judicial authorities in the Member States. The safeguards should also apply in the case of access and further use of the traffic data by authorities in other Member States.

35. In this context, the EDPS refers to initiatives for a new legal framework on data protection applicable to law enforcement (in the third pillar of the TEU). In his view, such a legal framework requires additional safeguards and could not limit itself to a reaffirmation of the general principles of data protection in the first pillar [1].

36. In the fourth place, there is a direct relationship between the adequacy of safety-measures and the costs of these measures. An adequate law on data retention must therefore contain incentives for the providers to invest in the technical infrastructure. Such an incentive could be that the providers are compensated for the additional costs of adequate safety-measures.

37. Summarised, adequate safety-measures should:

— limit the access to and further use of the data,

— provide for adequate technical and organisational safety-measures to protect the databases. This includes the adequate erasure of the data at the end of a retention

[1] See, in the same sense, the Position Paper on Law Enforcement and Information Exchange in the EU, adopted at the Spring Conference of European Data Protection Authorities, Krakow, 25 to 26 April 2005.

period and which acknowledges the demands for access and use by different groups of stakeholders,

— ensure the exercise of the rights of the data subjects, not just by reaffirming the general principles of data protection,

— contain incentives for the providers to invest in the technical infrastructure.

III The legal basis and the draft framework decision

38. The proposal is based on the EC Treaty, in particular Article 95 thereof, and aims, according to its Article 1, to harmonise the obligations for the providers with respect to the processing and retention of traffic and location data. It states that the data shall only be provided to the competent national authorities in individual cases, related to criminal offences, but it leaves the more precise definition of the purpose as well as the access to and the further use of the data to the discretion of the Member States, subject to the safeguards of the existing Community framework on data protection.

39. In this respect, the proposal has a more limited scope than the draft framework decision that is based on Article 31 (1)(c) TEU and that contains additional provisions on the access to the retained data as well as on requests for access from other Member States. The explanatory memorandum gives a justification of this limitation of the scope of the proposal. It states that access to and exchange of information between relevant law enforcement agencies is a matter which falls outside the scope of the EC Treaty.

40. The EDPS is not convinced by this statement in the explanatory memorandum. An intervention of the Community based on Article 95 EC (internal market) must have the removal of barriers to trade as its main object. According to the case-law of the Court of Justice, such an intervention must be genuinely appropriate for contributing to the removal of such a barrier. However, in its intervention the Community legislator must ensure the respect of fundamental rights (Article 6(2) TEU; see Section II of this opinion). For all that, the establishment on the Community level of rules on the retention of data in the interest of the internal market, may require that also the respect of fundamental rights is dealt with on the level of the European Community. If the Community legislator could not establish rules on the access and the use of data, it could not fulfil its obligation under Article 6 TEU since the latter rules are indispensable in order to ensure that data are retained with due respect to fundamental rights. In other words, according to the EDPS, the rules on the access, the use and the exchange of the data are inseparable from the obligation itself to retain the data.

41. As to the establishment of competent authorities, the EDPS admits that this is the responsibility of the Member States. Likewise is the organisation of the law enforcement and the judicial protection. However, a Community act can impose conditions on the Member States as to the designation of competent authorities, the judicial control or the access to justice by citizens. These provisions ensure that suitable mechanisms exist at a national level to guarantee the full effectiveness of the act, including the full compliance to data protection legislation.

42. The EDPS raises another point, related to the legal basis. It is up to the Community legislature to choose the adequate legal basis and, accordingly, the adequate legislative procedure. This choice goes beyond the mission of the EDPS. However, in the light of the important fundamental issues at stake, the EDPS expresses in the present situation a strong preference for the co-decision procedure. Only this procedure constitutes a transparent process of decision-making with full participation of the three institutions involved and with due respect to the principles on which the Union is founded.

IV The need for harmonisation

43. The proposal for a directive harmonises the types of data to be retained, the periods of time during which the data should be retained, as well as the purposes for which the data may be supplied to the competent authorities. The proposal envisages the full harmonisation of these elements. It is, in this respect, of a fundamentally different nature than the draft Framework Decision, which provides for minimum rules.

44. The EDPS underlines the need for full harmonisation of these elements, in view of the functioning of the internal market, the needs of law enforcement and — last but not least — the ECHR and the principles of data protection.

45. As to the functioning of the internal market, harmonisation of the obligations to retain data justifies the choice of the legal basis of the proposal (Article 95 EC). Allowing essential differences between the laws of the Member States would not take away the existing disturbances in the internal market of electronic communications which are *inter alia* due to the (imminent) adoption of legislative measures in Member States under Article 15 of Directive 2002/58/EC (see point 19 of this opinion).

46. This is even more important since to a notable amount of electronic communications, the jurisdiction of more than one Member State is relevant. Illustrative examples are: cross border phone calls, roaming, border crossing *during* mobile communications, and the use of a provider in another Member State than the country of residence of the individual.

47. Moreover, in this context lack of harmonisation would harm the needs of law enforcement, in so far as the competent authorities have to comply with different legal requirements. This could impede the exchange of information between the authorities of the Member States.

48. Finally, the EDPS emphasises — with a reference to his responsibility under Article 41 of Regulation (EC) No 45/2001 — that full harmonisation of the main elements included in the proposal is indispensable to comply with the ECHR and the principles of data protection. Any legislative measure that obliges to retain traffic and location data has to clearly limit the number of data to be retained, the periods of retention and (the purposes of) the access and further use of the data, in order to be acceptable from the perspective of data protection and to comply with the requirements of necessity and proportionality.

V Comments on the articles of the proposal

Article 3: Obligation to retain data

49. Article 3 is the key provision of the proposal. Article 3(1) introduces the obligation to retain traffic data and location data, whereas Article 3(2) gives effect to the principle of purpose limitation. Article 3(2) lays down three important limitations. The data retained shall only be provided:

— to the competent national authorities,

— in specific cases,

— for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.

Article 3(2) refers to the national legislation of the Member States for the specification of further limitations.

50. The EDPS welcomes Article 3(2) as an important provision but deems that the limitations are not precise enough, that the access and further use should explicitly be regulated under the directive and that additional safeguards are needed. As has been said in Section III of this opinion, the EDPS is not convinced that the non-inclusion of (precise) provisions on the access and the further use of the traffic and location data is an inevitable consequence of the legal base of the proposal (Article 95 EC). This leads to the following comments.

51. In the first place: it is not specified that other stakeholders, like the provider himself, do not have access to the data. Under Article 6 of Directive 2002/58/EC, providers may only process traffic data up to the end of the period the data are retained for billing purposes. According to the EDPS there is no justification for access by the providers or by other interested parties otherwise than the access foreseen under Directive 2002/58/EC, and subject to the conditions of that directive.

52. The EDPS recommends adding a provision in the text to ensure that individuals other than the competent authorities do not have access to the data. This provision could be formulated as follows: 'the data may only be accessed and/or processed for the purpose mentioned in Article 3(2)' or 'the providers shall effectively guarantee that access is only granted to the competent authorities'.

53. In the second place: the limitation to specific cases seems to prohibit routine access for 'fishing operations' or for data mining activities. However, the text of the proposal should specify that data can only be provided if this is needed in relation to a specific criminal offence.

54. In the third place: the EDPS welcomes the fact that the purpose of access is limited to serious criminal offences, such as terrorism and organised crime. In other less serious cases, access to traffic and location data will not easily be proportionate. However, the EDPS expresses doubts whether this limitation is precise enough, especially when access will be asked related to serious crime other than terrorism and organised crime. The practice in the Member States will diverge. The EDPS emphasised in section IV of this opinion the need of full harmonisation of the main elements included in the proposal. The EDPS recommends therefore limiting the provision to *certain* serious criminal offences.

55. In the fourth place: Contrary to the draft framework-decision, the proposal does not contain a provision on access. In the view of the EDPS, access to and further use of the data should not be ignored in the directive. They form an inseparable part of the subject-matter (see section III of this opinion).

56. The EDPS recommends the addition to the proposal of one or more articles on the access to the traffic and location data by the competent authorities and on the further use of the data. The objective of these articles should be to ensure that the data are only used for the purposes mentioned in Article 3(2), that the authorities ensure the quality, the confidentiality and the security of the data they have obtained and that the data will be erased when they are no longer

needed for the prevention, investigation, detection and prosecution of the specific criminal offence. Moreover, it should be laid down that access in specific cases should be under judicial control in the Member States.

57. In the fifth place: the proposal does not contain additional safeguards for data protection. The recitals simply refer to safeguards in existing legislation, more in particular Directive 95/46/EC and Directive 2002/58/EC. The EDPS disagrees with this limited approach of data protection in spite of the particular importance of (additional) safeguards (see section II of this opinion).

58. Therefore, the EDPS recommends including a paragraph on data protection. In this paragraph, the preceding recommendations concerning Article 3(2) could be inserted, as well as other provisions on data protection, such as provisions related to the exercise of his rights by the data subject (see section II of this opinion), to data quality and data security, and to traffic and location data of non suspects of criminal offences.

Article 4: Categories of data to be retained

59. In general, the EDPS welcomes the article and the annex, because of:

— the chosen legislative technique with functional descriptions in the body of the directive and technical details in an annex. It is flexible enough to respond adequately to technological developments and it gives legal certainty to the citizen,

— the distinction between data on telecommunications and Internet data, despite the fact that the distinction becomes technologically less important. From the perspective of data protection however, the distinction is important since on the Internet the borderline between content data and traffic data is not clear (see, for example, the recognition in Article 1(2) of the Directive that information consulted on the internet is content data),

— the level of harmonisation: the proposal envisages a high level of harmonisation with an exhaustive list of categories of data to be retained (as opposed to the draft Framework Decision that contains a minimum-list, with a wide margin for the Member States to add data). From the perspective of data protection, full harmonisation is essential (see section IV).

60. The EDPS recommends the following amendments:

— Article 4, second paragraph, should contain more substantial criteria to ensure that content data are not included. The following sentence should be added: 'The Annex may not include data that reveal the content of a communication',

— Article 5 opens up the possibility for the revision of the Annex by a Commission-directive ('comitology'). The EDPS advises that revisions of the Annex with a substantial impact on data protection should preferably be made by way of a directive, in accordance with the co-decision-procedure [1].

Article 7: Periods of retention

61. The EDPS welcomes the fact that the retention periods in the proposal are significantly shorter than the periods foreseen in the draft Framework decision:

— Remembering the doubts expressed in this opinion on the evidence of necessity of the retention of traffic data up to one year, the period of one year reflects the practices of law enforcement, *as they have been indicated* by the figures that have been provided by the Commission and the Presidency of the Council.

— These figures show as well that, except for exceptional cases, retention of data for longer periods does not reflect the practices of law enforcement.

— A shorter period of six months for data related to electronic communications taking place using solely or mainly the Internet protocol is important from the perspective of data protection, since the retention of Internet-communications results in vast databases (these data are usually not retained for billing purposes), the borderline with content data is vague and the retention for longer than six months does not reflect the practices of law enforcement.

62. It should be clarified in the text that:

— the retention periods of 6 months, respectively one year are maximum-periods of retention,

[1] See in the same sense, the Opinion of the EDPS of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (Paragraph 3.12).

— the data are erased at the end of the retention period. The text should also clarify how the data should be erased. According to the EDPS a provider has to erase the data by automated means, at least on a day by day basis.

Article 8: Storage requirements for retained data

63. This article is closely related to Article 3(2) and contains an important provision that can ensure that access in specific cases can be limited to data that are specifically needed. Articles 8 and 3(2) presuppose that the required data are transmitted by the providers to the authorities and that the latter do not have direct access to the databases. The EDPS recommends stating this presumption explicitly in the text.

64. The provision should be specified, by stating that:

— The required data are transmitted by the providers to the authorities (see point 63).

— The providers should install the necessary technical architecture, including search engines, to facilitate the targeted access to the specified data.

— The providers should ensure that only members of their staff with specified technical responsibilities have access to the databases for technical reasons and that those members of staff are aware of the sensitive character of the data and work under strict internal rules of confidentiality.

— The transmission of the data should not only take place without undue delay, but also without revealing other traffic and location data than the data needed for the purposes of the request.

Article 9: Statistics

65. The obligation for providers to supply statistics on a yearly basis helps the Community institutions to monitor the effectiveness of the implementation and application of the present proposal. Adequate information is needed.

66. According to the EDPS, this obligation gives effect to the principle of transparency. The European citizen is entitled to know how effective the data retention is. For this reason, the provider should additionally be obliged to keep logging lists and to perform systematic (self-) auditings, in order to enable the national data protection authorities to control the application of the rules on data protection in practice [1]. The proposal should be amended in that sense.

Article 10: Costs

67. As has been said in section II, there is a direct relationship between the adequacy of safety-measures and the costs of these measures, or in other words between security and costs. The EDPS therefore regards Article 10 — that provides for the reimbursement of demonstrated additional costs — as an important provision that could serve as an incentive for the providers to invest in the technical infrastructure.

68. According to the estimates in the Impact Assessment handed over by the Commission to the EDPS, the costs of data retention are considerable. For a large network and service provider, costs would be more than EUR 150 million, for a 12-month retention period, with annual operating costs of around EUR 50 million [2]. There are no figures, however, on costs of additional security measures, such as expensive search engines (see the comment on Article 6), nor on the (estimated) financial consequences of the full reimbursement of additional costs of the providers.

69. According to the EDPS more precise figures are needed, in order to be able to judge the proposal in its full extent. He suggests clarifying the financial consequences of the proposal in the explanatory memorandum.

70. As to the provision of Article 10 itself, the relationship between the adequacy of safety-measures and the costs should be made clear in the text of the provision. Moreover, the proposal should provide minimum-standards for the safety-measures to be taken by the providers, in order to be entitled to a reimbursement by a Member State. According to the EDPS, the determination of these standards could not be left

---

[1] See in the same sense, the Opinion of the EDPS of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (Paragraph 3.9).

[2] The Commission refers to figures of ETNO (the EU association of telecommunications operators) and to a report by MEP Alvaro on the draft Framework Decision.

completely to the Member States. This could prejudice the level of harmonisation envisaged by the directive. Furthermore, it should be taken into account that the Member States bear the financial consequences of the reimbursement.

Article 11: Amendment of Directive 2002/58/EC

71. The relation to Article 15(1) of Directive 2002/58/EC should be clarified, since this proposal deprives this provision of much of its content. The references in Article 15(1) of Directive 2002/58/EC to Article 6 and Article 9 (of that same directive) should be deleted, or at least be modified to clarify that the Member States are no longer competent to adopt legislation in relation to criminal offences, additional to the present proposal. Any ambiguity on their remaining competences — for instance as regards the retention of data for the purpose of 'not serious' criminal offences — must be taken away.

Article 12: Evaluation

72. The EDPS welcomes that the proposal contains an article on the evaluation of the Directive, within three years after its entry into force. An evaluation is all the more important in the perspective of the doubts on the necessity of the proposal, and of its proportionality.

73. In this perspective, the EDPS advises to provide for an even stricter obligation, that contains the following elements:

— The evaluation should comprise an assessment of the effectiveness of the implementation of the directive, from the perspective of law enforcement, as well as an assessment of the impact on the fundamental rights of the data subject. The Commission should include any evidence that could affect the evaluation.

— The evaluation should take place on a regular basis (at least every 2 years).

— The Commission should be obliged to submit amendments to the proposal, where appropriate (as in Article 18 of Directive 2002/58/EC).

VI Conclusions

Preconditions

74. It is essential to the EDPS that the proposal respects the fundamental rights. A legislative measure which would harm the protection guaranteed by Community law and more in particular by the case-law of the Court of Justice and the European Court of Human Rights is not only unacceptable, but also illegal.

75. The necessity and the proportionality of the obligation to retain data — in its full extent — have to be demonstrated.

76. As to the necessity: the EDPS recognises the changes of circumstances, but is as yet not convinced of the necessity of the retention of traffic and location data for law enforcement purposes, as established in the proposal.

77. Nevertheless, the EDPS presents in this opinion his view on the proportionality of the proposal. This means in the first place, retention of traffic and location data alone is in itself not an adequate or effective response. Additional measures are needed, so as to ensure that the authorities have a targeted and quick access to the data needed in a specific case. In the second place, the proposal should:

— limit the retention periods. The periods must reflect the needs of law enforcement,

— limit the number of data to be stored. This number must reflect the needs of law enforcement and ensure that access to content data is not possible,

— contain adequate safety measures.

General appraisal

78. The EDPS underlines the importance of the fact that the present text of the proposal foresees a full harmonisation of the main elements of the proposal, in particular the types of data to be retained, the periods of time during which the data should be retained, as well as (the purposes of) the access and further use of the data.

79. On some points, further clarifications are needed, for instance to ensure the adequate erasure of the data at the end of a retention period and to effectively prevent access and use by different groups of stakeholders.

80. The EDPS considers the following points essential, for the proposal to be acceptable from the perspective of data protection:

— The addition to the proposal of specific provisions on access to the traffic and location data by the competent authorities and on the further use of the data, as an essential and inseparable part of the subject-matter.

— The addition to the proposal of further additional safeguards for data protection (contrary to a simply reference to safeguards in existing legislation, more in particular Directive 95/46/EC and Directive 2002/58/EC), *inter alia* to ensure the exercise of the rights of the data subjects.

— The addition to the proposal of further incentives to the providers to invest in an adequate technical infrastructure, including financial incentives. This infrastructure can only be adequate in so far as effective search engines exist.

Recommendations for modifications of the proposal

81. As to Article 3(2):

— addition of a provision to ensure that individuals other than the competent authorities do not have access to the data. This provision could be formulated as follows: 'the data may only be accessed and/or processed for the purpose mentioned in Article 3(2)' or 'the providers shall effectively guarantee that access is only granted to the competent authorities':

— specification that data can only be provided if this is needed in relation to a specific criminal offence,

— limitation of the provision to *certain* serious criminal offences,

— addition to the proposal of one or more articles on the access to the traffic and location data by the competent authorities and on the further use of the data, as well as of a provision that access in specific cases should be under judicial control in the Member States,

— inclusion of a paragraph on data protection.

82. As to Articles 4 and 5:

— addition to Article 4, second paragraph, of the following sentence: 'The Annex may not include data that reveal the content of a communication',

— specification that revisions of the Annex with a substantial impact on data protection should preferably be made by way of a directive, in accordance with the co-decision procedure.

83. As to Article 7, a specification in the text that the:

— retention periods of 6 months and one year are maximum-periods of retention,

— data are erased at the end of the retention period. The text should also clarify how the data should be erased, namely by the provider by automated means, at least on a day by day basis.

84. As to Article 8, a specification in the text that:

— the required data are transmitted by the providers to the authorities,

— the providers should install the necessary technical architecture, including search engines, to facilitate the targeted access to the specified data,

— the providers should ensure that only members of their staff with specified technical responsibilities have access to the databases for technical reasons and that those members of staff are aware of the sensitive character of the data and work under strict internal rules of confidentiality,

— the transmission of the data should not only take place without undue delay, but also without revealing other traffic and location data than the data needed for the purposes of the request.

85. As to Article 9:

— addition of a provision that obliges the provider to keep logging lists and to perform systematic (self-) auditings, in order to enable the national data protection authorities to control the application of the rules on data protection in practice.

86. As to Article 10:

— clarification of the relationship between the adequacy of safety-measures and the costs should be made clear in the text of the provision,

— addition of minimum-standards for the safety-measures to be taken by the providers, in order to be entitled to a reimbursement by a Member State,

— clarification of the financial consequences of the proposal in the explanatory memorandum.

87. As to Article 11:

— amendment of Article 15 (1) of Directive 2002/58/EC to delete the references to Article 6 and Article 9 (of that same directive), or at least to modify them in order to clarify that the Member States are no longer competent to adopt legislation in relation to criminal offences, additional to the present proposal.

88. As to Article 12, amendment of the provision of evaluation:

— it should comprise an assessment of the effectiveness of the implementation of the directive,

— it should take place on a regular basis (at least every 2 years),

— the Commission should be obliged to submit amendments to the proposal, where appropriate (like in Article 18 of Directive 2002/58/EC).

Done at Brussels on 26 September 2005.

Peter HUSTINX,
European Data Protection Supervisor

I

(Meddelelser)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om forslaget til Europa-Parlamentets og Rådets direktiv om opbevaring af data, der behandles i forbindelse med levering af offentlige elektroniske kommunikationstjenester og om ændring af direktiv 2002/58/EF (KOM(2005) 438 endelig)

(2005/C 298/01)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

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

som henviser til EU-chartret 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] og til Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation) [2],

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 [3] , særlig artikel 41, og

som henviser til Kommissionens anmodning om udtalelse, jf. artikel 28, stk. 2, i forordning (EF) nr. 45/2001, modtaget den 23. september 2005,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. Indledning

1. Den tilsynsførende glæder sig over at blive hørt på grundlag af artikel 28, stk. 2, i forordning (EF) nr. 45/2001. Men det er klart, at denne udtalelse skal nævnes i direktivets præambel, da artikel 28, stk. 2, i forordning (EF) nr. 45/2001 er bindende.

2. Den tilsynsførende erkender, at det er vigtigt for medlemsstaternes retshåndhævende myndigheder at have alle de nødvendige juridiske instrumenter til deres rådighed,

[1] EFT L 281 af 23.11.1995, s. 31.

[2] EFT L 201 af 31.7.2002, s. 37.

[3] EFT L 8 af 12.1.2001, s. 1.

navnlig i bekæmpelsen af terrorisme og anden grov kriminalitet. Tilstrækkelig adgang til visse trafik- og lokaliseringsdata hos offentlige elektroniske tjenester kan være et afgørende instrument for de retshåndhævende myndigheder og kan bidrage til personers fysiske sikkerhed. Samtidig gøres der opmærksom på, at dette ikke automatisk indebærer, at de nye instrumenter, der er omhandlet i forslaget, er nødvendige.

3. Det er også klart, at forslaget har en betydelig indvirkning på beskyttelsen af personoplysninger. Hvis man udelukkende betragter forslaget ud fra et databeskyttelsessynspunkt, bør trafik- og lokaliseringsdata slet ikke opbevares med henblik på retshåndhævelse. Det er af hensyn til databeskyttelsen, at direktiv 2002/58/EF fastsætter som retsprincip, at trafikdata skal slettes, så snart lagring ikke længere er nødvendig i forbindelse med selve kommunikationen (bl.a. med henblik på debitering). Fravigelse af dette princip er underlagt strenge betingelser.

4. I denne udtalelse vil den tilsynsførende fremhæve forslagets indvirkning på beskyttelsen af personoplysninger. Den tilsynsførende vil desuden tage hensyn til, at forslaget, uanset dets betydning for retshåndhævelse, ikke må medføre, at personer fratages deres grundlæggende ret til beskyttelse af privatlivets fred.

5. Denne udtalelse fra den tilsynsførende skal ses i lyset af disse betragtninger. Den tilsynsførende vil anvende en afbalanceret tilgang, hvori behovet for og proportionaliteten i et indgreb i databeskyttelsen spiller en central rolle.

6. For så vidt angår selve forslaget skal det ses som en reaktion på initiativet fra Den Franske Republik, Irland, Kongeriget Sverige og Det Forenede Kongerige til en rammeafgørelse om opbevaring af data, der behandles og lagres i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester, og af data, der findes i offentlige kommunikationsnet, med henblik på at forebygge, efterforske, afsløre og strafforfølge kriminalitet og strafbare handlinger, herunder terrorisme (»udkastet til rammeafgørelse«), som Europa-Parlamentet har forkastet (under høringsproceduren).

7. Den tilsynsførende er ikke blevet hørt om udkastet til rammeafgørelse og har heller ikke afgivet udtalelse på eget initiativ. Den tilsynsførende agter ikke at afgive udtalelse om udkastet til rammeafgørelse på nuværende tidspunkt, men vil i nærværende udtalelse henvise til dette udkast, når han finder det hensigtsmæssigt.

II. Generelle bemærkninger

Forslagets indvirkning på beskyttelsen af personoplysninger

8. Den tilsynsførende finder det afgørende, at forslaget respekterer de grundlæggende rettigheder. En lovgivning, der ville skade den beskyttelse, som er sikret ved fællesskabsretten og mere specifikt ved Domstolens og Den Europæiske Menneskerettighedsdomstols retspraksis, er ikke alene uacceptabel, men også ulovlig. Forholdene i samfundet kan have ændret sig på grund af terrorangreb, men dette må ikke medføre, at høje beskyttelsesstandarder i retsstaten anfægtes. Beskyttelsen er lovfæstet uanset de reelle behov for retshåndhævelse. Desuden giver retspraksis mulighed for undtagelser, hvis de er nødvendige i et demokratisk samfund.

9. Forslaget har direkte indvirkning på beskyttelsen i henhold til artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (EMRK). Følgende fremgår af Den Europæiske Menneskerettighedsdomstols retspraksis:

— Lagring af oplysninger om enkeltpersoner betragtes som et indgreb i privatlivets fred, selv om de ikke indeholder følsomme data (Amann [1]).

— Det samme gælder praksis med at 'aflæse' telefonsamtaler, som indebærer brugen af en anordning, der automatisk registrerer de kaldte telefonnumre og tidspunktet og taletiden for hver samtale (Malone [2]).

— Begrundelsen for indgreb skal veje tungere end den negative virkning, som selve eksistensen af de pågældende lovbestemmelser kunne have for de registrerede (Dudgeon [3]).

10. Det hedder i artikel 6, stk. 2, i EU-traktaten, at Unionen respekterer de grundlæggende rettigheder, således som de garanteres ved EMRK. Det fremgår af punkt 9, at pligten til at opbevare data i henhold til Den Europæiske Menneskerettighedsdomstols retspraksis falder ind under artikel 8 i EMRK, og at der kræves en stærk begrundelse, som opfylder kriteriet i

---

([1]) Den Europæiske Menneskerettighedsdomstols dom af 16. februar 2000, Amann, 2000-II, beg. 27798/95.

([2]) Den Europæiske Menneskerettighedsdomstols dom af 2. august 1984, Malone, A82, beg. 8691/79.

([3]) Den Europæiske Menneskerettighedsdomstols dom af 22. oktober 1981, Dudgeon, A45, beg. 7525/76.

Dudgeon-dommen. Behovet for og proportionaliteten i pligten til at opbevare — samtlige — data skal godtgøres.

11. Desuden indvirker forslaget kraftigt på de databeskyttelsesprincipper, der er anerkendt i fællesskabsretten, på følgende områder:

— Dataene skal opbevares i en periode, der er meget længere end de perioder, der normalt gælder for opbevaring hos udbydere af offentligt tilgængelige elektroniske kommunikationstjenester eller i et offentligt kommunikationsnet (begge i det følgende benævnt »udbydere«).

— I henhold til direktiv 2002/58/EF, nærmere bestemt artikel 6, kan data kun indsamles og lagres af grunde, der har direkte forbindelse med selve kommunikationen, bl.a. debitering ([1]). Derefter skal dataene slettes (med visse undtagelser). I henhold til forslaget er opbevaring med henblik på strafferetlig retshåndhævelse obligatorisk. Udgangspunktet er altså det modsatte.

— Direktiv 2002/58/EF garanterer sikkerhed og datahemmelighed. Forslaget må ikke medføre lakuner på dette område; der skal være strenge garantier, og formålsbegrænsningen skal være klarere.

— Indførelsen af pligten til at opbevare data som fastsat i forslaget fører til omfattende databaser og indebærer særlige risici for den registrerede. Man kunne forestille sig kommerciel anvendelse af dataene og retshåndhævende myndigheders eller nationale sikkerhedstjenesters anvendelse af dataene til »fiskeekspeditioner« og/eller »data mining«.

12. Endelig er både beskyttelse af privatlivets fred og beskyttelse af personoplysninger anerkendt i charteret om grundlæggende rettigheder som nævnt i begrundelsen.

13. Forslagets indvirkning på beskyttelsen af personoplysninger skal analyseres indgående. I denne analyse vil den tilsynsførende tage hensyn til ovennævnte elementer og vil konkludere, at der er behov for flere garantier. En henvisning til det gældende lovgrundlag vedrørende databeskyttelse (navnlig direktiv 95/46/EF og 2002/58/EF) er ikke nok.

Behovet for opbevaring af trafik- og lokaliseringsdata

14. Den tilsynsførende minder om Databeskyttelsesgruppens konklusion af 9. november 2004 om udkastet til rammeafgørelse. Gruppen erklærede, at obligatorisk opbevaring af trafikdata på de betingelser, der er fastsat i udkastet til rammeafgørelse, ikke er acceptabel. Denne konklusion byggede bl.a. på, at det ikke var godtgjort, at der er behov for at opbevare data af hensyn til ordre public, da en analyse viste, at de fleste af de trafikdata, som retshåndhævende myndigheder har bedt om, ikke har været mere end et halvt år gamle.

15. Den tilsynsførende mener, at Databeskyttelsesgruppens betragtninger bør være udgangspunktet for vurderingen af forslaget. Resultaterne af disse betragtninger kan dog ikke bare omsættes i forslaget. Der skal tages hensyn til, at forholdene kan ændre sig. Den tilsynsførende mener, at den udvikling, der beskrives i det følgende, kunne være relevant for vurderingen.

16. For det første er der blevet fremlagt nogle tal for at påvise, at retshåndhævende myndigheder i praksis beder om trafikdata, der er op til et år gamle. Kommissionen og Rådets formandskab lægger vægt på en undersøgelse foretaget af Det Forenede Kongeriges politi ([2]), der viser, at 85 % af de trafikdata, som politiet har bedt om, ganske vist var under et halvt år gamle, men at data, der er et halvt til et helt år gamle, er blevet anvendt i komplicerede efterforskninger af grovere kriminalitet. Der er også blevet givet nogle eksempler på sager. Opbevaringsperioden i forslaget — et år for telefondata — afspejler denne retshåndhævelsespraksis.

17. Den tilsynsførende er ikke overbevist om, at disse tal taler for, at trafikdata skal opbevares i op til et år. Det forhold, at adgangen til trafik- og/eller lokaliseringsdata i nogle tilfælde var medvirkende til, at en forbrydelse blev opklaret, betyder ikke automatisk, at disse data (generelt) er nødvendige som et redskab i retshåndhævelsen. Man bør dog ikke ignorere disse tal. De er i det mindste et seriøst forsøg på at påvise behovet for opbevaring. Desuden fremgår det klart af tallene, at en opbevaringsperiode på over et år ikke er nødvendig med den nuværende retshåndhævelsespraksis.

18. For det andet benytter udbyderne ikke altid de muligheder, de har i henhold til direktiv 2002/58/EF for at opbevare trafikdata med henblik på debitering, da der i et stigende antal tilfælde slet ikke sker dataopbevaring med henblik på debitering (taletidskort til mobilkommunikation, fastprisabon-

([1]) Se også punkt 3 i denne udtalelse.

([2]) Liberty and security, striking the right balance. Dokument fra Det Forenede Kongeriges EU-formandskab af 7. september 2005.

nementer osv.). I disse tilfælde — som i praksis er blevet hyppigere — vil trafik- og lokaliseringsdata slet ikke blive lagret, men slettet straks efter kommunikationen. Det samme gælder for opkald, der ikke går igennem. Dette kan have indflydelse på retshåndhævelsens effektivitet.

19. Desuden kan denne udvikling i teletjenester føre til forstyrrelser i det indre markeds funktion, bl.a. på grund af (den nært forestående) vedtagelse af lovgivning i medlemsstaterne i henhold til artikel 15 i direktiv 2002/58/EF. F.eks. offentliggjorde den italienske regering for nylig et dekret, hvorefter udbydere skal lagre telefondata i fire år. Denne pligt vil medføre betydelige udgifter i visse medlemsstater, f.eks. Italien.

20. For det tredje har de retshåndhævende myndigheders arbejdsmetoder også udviklet sig, idet proaktiv efterforskning og brugen af tekniske hjælpemidler har fået større betydning. Denne udvikling betyder, at myndighederne skal råde over tilstrækkelige og præcist formulerede redskaber, således at de kan udføre deres arbejde under behørig hensyntagen til databeskyttelsesprincipperne. Et af de redskaber, myndighederne i medlemsstaterne som regel råder over, er hastesikring af data eller fastfrysning af kommunikationsdata efter anmodning i en konkret efterforskning. Det er blevet anført, at dette redskab, der i sig selv har mindre indvirkning på principperne end det, der nu foreslås (dataopbevaring), måske ikke altid er nok, især ikke til at spore personer, der er indblandet i terrorisme eller anden grov kriminalitet, og som ikke tidligere har været mistænkt for kriminel virksomhed. Der skal dog fremlægges flere beviser, før man kan afgøre, om det virkelig er tilfældet.

21. For det fjerde er bekymringen for terrorangreb blevet større. Den tilsynsførende er enig i det synspunkt, der er fremført i forbindelse med forslagene om dataopbevaring, at fysisk sikkerhed i sig selv er af altovervejende betydning. Samfundet skal beskyttes. Derfor er regeringerne nødt til i tilfælde af angreb på samfundet at vise, at de tager seriøst hensyn til dette behov for beskyttelse, og til at undersøge, om de skal reagere ved at indføre ny lovgivning. Det er klart, at den tilsynsførende fuldt ud støtter regeringernes opgaver — både på nationalt og på europæisk plan — med at beskytte samfundet og vise, at de gør alt, hvad der er nødvendigt for at yde beskyttelse, herunder vedtagelse af nye, legitime og effektive foranstaltninger på baggrund af deres undersøgelser.

22. Den tilsynsførende erkender, at forholdene ændrer sig, men er endnu ikke overbevist om, at det er nødvendigt at opbevare trafik- og lokaliseringsdata med henblik på retshåndhævelse som fastsat i forslaget. Han understreger betydningen af retsprincippet i direktiv 2002/58/EF om, at trafikdata skal slettes, så snart lagring ikke længere er nødvendig til formål, der ikke har forbindelse med selve kommunikationen. Desuden beviser de fremlagte tal ikke, at det nuværende lovgrundlag ikke sikrer de instrumenter, der er nødvendige for at beskytte den fysiske sikkerhed, eller at medlemsstaterne fuldt ud anvender deres beføjelser i henhold til europæisk ret til at samarbejde, således som de er fastsat i det nuværende lovgrundlag (men uden de nødvendige resultater).

23. Hvis Europa-Parlamentet og Rådet — efter en omhyggelig afvejning af de interesser, der er på spil — imidlertid drager den konklusion, at behovet for opbevaring af trafik- og lokaliseringsdata er tilstrækkeligt påvist, mener den tilsynsførende, at opbevaringen kun kan forsvares i henhold til fællesskabsretten, hvis proportionalitetsprincippet respekteres, og der gives tilstrækkelige garantier i overensstemmelse med denne udtalelse.

Proportionalitet

24. Proportionaliteten i forslaget til ny lovgivning afhænger af substansen i de bestemmelser, den indeholder: Indeholder den tilstrækkelige bestemmelser, der står i et rimeligt forhold til samfundets behov?

25. Den første betragtning vedrører forslagets tilstrækkelighed: Kan man forvente, at forslaget øger EU-borgernes fysiske sikkerhed? En grund til at betvivle tilstrækkeligheden, som ofte nævnes i den offentlige debat, er, at trafik- og lokaliseringsdata ikke altid er knyttet til en bestemt person, således at viden om et telefonnummer (eller et IP-nummer) ikke nødvendigvis afslører en persons identitet. En anden — og endnu mere alvorlig — grund til tvivl er, om retshåndhævende myndigheder har mulighed for let at finde, hvad de skal bruge i en bestemt sag, hvis databaserne bliver gigantiske.

26. Den tilsynsførende mener, at opbevaring af trafik- og lokaliseringsdata ikke i sig selv er et tilstrækkeligt eller effektivt tiltag. Der er behov for yderligere foranstaltninger for at sikre, at myndighederne har en målrettet og hurtig adgang til de data, som de har brug for i en bestemt sag. Opbevaring af data er kun tilstrækkelig og effektiv, hvis der findes effektive søgemaskiner.

27. Den anden betragtning er, om bestemmelserne står i et rimeligt forhold til behovene. For at dette er tilfældet, skal forslaget

— begrænse opbevaringsperioderne. Perioderne skal afspejle de påviste behov for retshåndhævelse

— begrænse antallet af data, der skal lagres. Dette antal skal afspejle de påviste behov for retshåndhævelse, og det skal sikres, at der ikke er adgang til indholdsdata

— indeholde tilstrækkelige sikkerhedsforanstaltninger, således at adgangen og yderligere anvendelse begrænses, dataenes sikkerhed garanteres, og det sikres, at de registrerede selv kan udøve deres rettigheder.

28. Den tilsynsførende understreger betydningen af disse strenge begrænsninger med tilstrækkelige garantier med henblik på begrænset adgang. Han mener, at under hensyn til betydningen af de tre elementer, der er nævnt i punkt 27, må medlemsstaterne ikke træffe yderligere nationale foranstaltninger med hensyn til disse tre elementer, der anfægter proportionaliteten. Dette behov for harmonisering behandles i afsnit IV.

Tilstrækkelige sikkerhedsforanstaltninger

29. Forslagets virkning bliver, at udbyderne kommer til at råde over databaser, hvor en stor mængde trafik- og lokaliseringsdata oplagres.

30. For det første skal forslaget sikre, at adgangen til og den videre anvendelse af disse data begrænses til kun at være mulig under bestemte omstændigheder og til et begrænset antal bestemte formål.

31. For det andet skal databaserne være tilstrækkeligt beskyttet (datasikkerhed). Med henblik herpå skal det sikres, at dataene slettes effektivt, når opbevaringsperioderne udløber. Der må ikke ske »datadumping« eller dataudnyttelse. Dette kræver kort sagt en høj datasikkerhed og tilstrækkelige tekniske og organisatoriske sikkerhedsforanstaltninger.

32. En høj datasikkerhed er så meget vigtigere, som der kunne komme anmodninger om adgang og anvendelse fra mindst følgende tre grupper interessenter, blot fordi dataene findes:

— udbyderne selv. De kunne blive fristet til at anvende dataene til deres egne kommercielle formål. Der skal være garantier, der forhindrer kopiering af disse filer

— retshåndhævende myndigheder. Forslaget giver dem ret til adgang, men kun i bestemte tilfælde og efter national ret (forslagets artikel 3, stk. 2). Der bør ikke være adgang til »data mining« eller »fiskeekspeditioner«. Der skal være klare regler for udvekslingen af data med andre medlemsstaters myndigheder

— efterretningstjenester (med ansvar for national sikkerhed).

33. Med hensyn til adgang for efterretningstjenester gør den tilsynsførende opmærksom på, at tiltag under søjle 3 og søjle 1 i henhold til artikel 33 i TEU og artikel 64 i TEF ikke er til hinder for, at medlemsstaterne kan udøve deres beføjelser med hensyn til opretholdelse af lov og orden og beskyttelse af den indre sikkerhed. Den tilsynsførende mener, at disse bestemmelser har den virkning, at Den Europæiske Union ikke har kompetence til at styre sikkerheds- eller efterretningstjenesters adgang til de data, som udbyderne opbevarer. Med andre ord er hverken disse tjenesters adgang til udbyderens trafik- og lokaliseringsdata eller den videre anvendelse af de oplysninger, som disse tjenester skaffer, berørt af EU-lovgivningen. Det er et element, der skal tages i betragtning i vurderingen af forslaget. Det er medlemsstaterne, der skal træffe de nødvendige foranstaltninger til at regulere efterretningstjenesters adgang.

34. For det tredje kan de virkninger, der er beskrevet i punkt 33, have potentielle følger for den registrerede. Der er behov for yderligere garantier for at sikre, at han nemt og hurtigt kan udøve sine rettigheder som registreret. Den tilsynsførende gør opmærksom på, at der skal indføres en effektiv kontrol med adgang og videre anvendelse, der helst skal foretages af retsmyndigheder i medlemsstaterne. Garantierne skal også gælde for myndigheder i andre medlemsstater i forbindelse med deres adgang til og videre anvendelse af trafikdata.

35. I den forbindelse henviser den tilsynsførende til initiativer til et nyt lovgrundlag vedrørende databeskyttelse, der skal gælde i forbindelse med retshåndhævelse (under søjle 3 i TEU). Han mener, at dette lovgrundlag kræver yderligere garantier og ikke kun må have form af en fornyet bekræftelse af de generelle databeskyttelsesprincipper under søjle 1 ([1]).

36. For det fjerde er der en direkte forbindelse mellem tilstrækkelige sikkerhedsforanstaltninger og udgifterne hertil. En tilstrækkelig lovgivning om dataopbevaring skal derfor indeholde incitamenter for udbyderne til at investere i den tekniske infrastruktur. Et sådant incitament kunne være, at udbyderne får deres ekstraudgifter til tilstrækkelige sikkerhedsforanstaltninger godtgjort.

37. Tilstrækkelige sikkerhedsforanstaltninger kan sammenfattes således:

— De skal begrænse adgangen til og videre anvendelse af dataene.

— Der skal være tilstrækkelige tekniske og organisatoriske sikkerhedsforanstaltninger til at beskytte databaserne. Dette omfatter, at data skal slettes på en tilstrækkelig måde, når opbevaringsperioden udløber, og at der i den

([1]) Se i denne forbindelse det oplæg om retshåndhævelse og informationsudveksling i EU, der blev vedtaget på de europæiske databeskyttelsesmyndigheders forårskonference i Krakow den 25.-26. april 2005.

forbindelse skal tages hensyn til anmodninger om adgang og anvendelse fra forskellige grupper af interessenter.

— Det skal sikres, at de registrerede kan udøve deres rettigheder, og ikke kun ved, at de generelle databeskyttelsesprincipper bekræftes på ny.

— De skal indeholde incitamenter til udbyderne til at investere i den tekniske infrastruktur.

III. Retsgrundlaget og udkastet til rammeafgørelse

38. Forslaget er baseret på EF-traktaten, særlig artikel 95, og har i henhold til artikel 1 til formål at harmonisere udbydernes forpligtelser i forbindelse med behandlingen og opbevaringen af trafik- og lokaliseringsdata. Det bestemmer, at dataene kun udleveres til de kompetente nationale myndigheder i enkelttilfælde, der vedrører lovovertrædelser, men det overlades til medlemsstaterne at fastlægge formålet og tage stilling til adgangen til og den videre anvendelse af dataene, dog med de garantier, der findes i det gældende EF-lovgrundlag vedrørende databeskyttelse.

39. I den henseende har forslaget et mere begrænset anvendelsesområde end udkastet til rammeafgørelse, der er baseret på artikel 31, stk. 1, litra c), i TEU, og som indeholder yderligere bestemmelser om adgangen til de opbevarede data og om anmodninger om adgang fra andre medlemsstater. Begrundelsen indeholder en forklaring på denne begrænsning af forslagets anvendelsesområde. Det anføres, at adgang til og udveksling af oplysninger mellem de relevante retshåndhævende myndigheder er et spørgsmål, der falder uden for EF-traktatens anvendelsesområde.

40. Den tilsynsførende finder ikke denne forklaring i begrundelsen overbevisende. Et tiltag fra Fællesskabets side på grundlag af artikel 95 i TEF (det indre marked) skal have til hovedformål at fjerne handelshindringer. I henhold til Domstolens retspraksis skal et sådant tiltag være virkelig velegnet til at bidrage til fjernelse af sådanne hindringer. Fællesskabslovgiveren skal dog respektere de grundlæggende rettigheder i sit tiltag (artikel 6, stk. 2, i TEU; se afsnit II i denne udtalelse). En indførelse af regler om dataopbevaring på fællesskabsplan af hensyn til det indre marked kan alligevel medføre, at der også tages hensyn til respekten for de grundlæggende rettigheder på fællesskabsplan. Hvis fællesskabslovgiveren ikke kunne fastsætte regler om adgang til og anvendelse af data, kunne pligten i henhold til artikel 6 i TEU ikke opfyldes, da disse regler er uundværlige for at sikre, at data opbevares med behørig respekt for de grundlæggende rettigheder. Med andre ord mener den tilsynsførende, at reglerne om adgang til og anvendelse og udveksling af data er uløseligt forbundet med selve pligten til at opbevare dataene.

41. Med hensyn til fastlæggelse af kompetente myndigheder erkender den tilsynsførende, at det er medlemsstaternes ansvar. Det samme gælder tilrettelæggelsen af retshåndhævelse og domstolsbeskyttelse. En fællesskabsretsakt kan dog pålægge medlemsstaterne betingelser for udpegelsen af kompetente myndigheder, domstolskontrollen eller borgernes adgang til klage og domstolsprøvelse. Disse bestemmelser sikrer, at der findes passende ordninger på nationalt plan til at sikre, at retsakten bliver helt effektiv, bl.a. at databeskyttelseslovgivningen overholdes fuldt ud.

42. Den tilsynsførende rejser et andet punkt vedrørende retsgrundlaget. Det er op til fællesskabslovgiveren at vælge et passende retsgrundlag og dermed en passende lovgivningsprocedure. Dette valg falder uden for den tilsynsførendes opgave. På baggrund af de vigtige fundamentale spørgsmål, der er på spil, foretrækker den tilsynsførende dog i den nuværende situation langt den fælles beslutningsprocedure. Kun denne procedure udgør en gennemsigtig beslutningsproces med fuld deltagelse af de tre berørte institutioner og med behørig respekt for de principper, som EU bygger på.

IV. Behovet for harmonisering

43. Direktivforslaget harmoniserer de typer data, der skal opbevares, opbevaringsperioderne samt de formål, hvortil dataene kan udleveres til de kompetente myndigheder. Forslaget tager sigte på fuld harmonisering af disse elementer. Det er i den henseende fundamentalt forskelligt fra udkastet til rammeafgørelse, som indeholder minimumsregler.

44. Den tilsynsførende understreger, at der skal ske fuld harmonisering af disse elementer af hensyn til det indre markeds funktion, retshåndhævelsesbehovene og — sidst men ikke mindst — EMRK og databeskyttelsesprincipperne.

45. Med hensyn til det indre markeds funktion er en harmonisering af forpligtelserne til at opbevare data begrundelsen for valget af retsgrundlag for forslaget (artikel 95 i TEF). Hvis der tillades væsentlige forskelle mellem medlemsstaternes love, vil man ikke fjerne de nuværende forstyrrelser på det indre marked for elektronisk kommunikation, der bl.a. skyldes (den nært forestående) vedtagelse af lovgivning i medlemsstaterne i henhold til artikel 15 i direktiv 2002/58/EF (se punkt 19 i denne udtalelse).

46. Dette er så meget vigtigere, som mere end én medlemsstats kompetence er relevant i forbindelse med store dele af den elektroniske kommunikation. Eksempler herpå er telefonsamtaler over grænserne, roaming, grænsepassage *under* mobilkommunikation og brugen af en udbyder i en anden medlemsstat end den pågældendes bopælsland.

47. Desuden ville manglende harmonisering i denne forbindelse gå ud over retshåndhævelsesbehovene, da de kompetente myndigheder skal opfylde forskellige retskrav. Dette kunne hindre informationsudvekslingen mellem medlemsstaternes myndigheder.

48. Endelig understreger den tilsynsførende — med henvisning til sin opgave i henhold til artikel 41 i forordning (EF) nr. 45/2001 — at en harmonisering af hovedelementerne i forslaget er nødvendig for at overholde EMRK og databeskyttelsesprincipperne. En lovgivning, hvorefter trafik- og lokaliseringsdata skal opbevares, skal klart begrænse antallet af data, der skal opbevares, opbevaringsperioderne og (formålet med) adgangen til og videre anvendelse af dataene for at være acceptabel ud fra et databeskyttelsessynspunkt og skal opfylde kravene om nødvendighed og proportionalitet.

V. Bemærkninger til forslagets artikler

Artikel 3: Forpligtelse til at opbevare data

49. Artikel 3 er forslagets centrale bestemmelse. Artikel 3, stk. 1, indfører pligten til at opbevare trafik- og lokaliseringsdata, medens stk. 2 gennemfører princippet om formålsbegrænsning. Artikel 3, stk. 2, fastsætter tre vigtige begrænsninger. De opbevarede data må kun udleveres

— til de kompetente nationale myndigheder

— i bestemte tilfælde

— med henblik på at forebygge, efterforske, afsløre og strafforfølge grov kriminalitet såsom terrorisme og organiseret kriminalitet.

Artikel 3, stk. 2, henviser til medlemsstaternes nationale lovgivning med hensyn til fastsættelse af nærmere begrænsninger.

50. Den tilsynsførende ser med tilfredshed på artikel 3, stk. 2, som en vigtig bestemmelse, men mener ikke, at begrænsningerne er præcise nok, da direktivet bør indeholde udtrykkelige bestemmelser om adgang og videre anvendelse, og der er behov for yderligere garantier. Som nævnt i afsnit III i denne udtalelse er den tilsynsførende ikke overbevist om, at manglende (præcise) bestemmelser om adgangen til og den videre anvendelse af trafik- og lokaliseringsdata er en uundgåelig følge af forslagets retsgrundlag (artikel 95 i TEF). Dette giver anledning til følgende bemærkninger:

51. For det første er det ikke fastsat, at andre interessenter, som udbyderen selv, ikke har adgang til dataene. I henhold til artikel 6 i direktiv 2002/58/EF må udbydere kun behandle trafikdata indtil udløbet af fristen for opbevaring med henblik på debitering. Den tilsynsførende mener ikke, at der er nogen begrundelse for, at udbyderne eller andre interesserede parter skal have anden adgang end den, der er fastsat i direktiv 2002/58/EF, og på direktivets betingelser.

52. Den tilsynsførende anbefaler, at der tilføjes en bestemmelse i teksten for at sikre, at ikke andre end de kompetente myndigheder har adgang til dataene. Denne bestemmelse kunne affattes således: »Der gives kun mulighed for adgang til og/eller behandling af dataene til det formål, der er nævnt i artikel 3, stk. 2« eller »Udbyderne skal effektivt sikre, at kun de kompetente myndigheder får adgang«.

53. For det andet synes begrænsningen til bestemte tilfælde at forhindre rutineadgang med henblik på »fiskeekspeditioner« eller »data mining«. Forslaget bør dog bestemme, at data kun kan udleveres, hvis det er nødvendigt i forbindelse med en specifik lovovertrædelse.

54. For det tredje er den tilsynsførende godt tilfreds med, at formålet med adgang er begrænset til grov kriminalitet såsom terrorisme og organiseret kriminalitet. I andre mindre alvorlige tilfælde vil det ofte være urimeligt at give adgang til trafik- og lokaliseringsdata. Den tilsynsførende tvivler dog på, at denne begrænsning er præcis nok, især når der anmodes om adgang i forbindelse med andre former for grov kriminalitet end terrorisme og organiseret kriminalitet. Praksis i medlemsstaterne vil være forskellig. Den tilsynsførende understreger i afsnit IV i denne udtalelse, at der skal ske fuld harmonisering af forslagets hovedelementer. Den tilsynsførende anbefaler derfor, at udlevering kun skal ske i forbindelse med *visse former for* grov kriminalitet.

55. For det fjerde indeholder forslaget i modsætning til udkastet til rammeafgørelse ikke nogen bestemmelse om adgang. Den tilsynsførende mener, at adgang til og videre anvendelse af dataene skal være omhandlet i direktivet. De er uløseligt forbundet med emnet (se afsnit III i denne udtalelse).

56. Den tilsynsførende anbefaler, at der i forslaget tilføjes en eller flere artikler om de kompetente myndigheders adgang til trafik- og lokaliseringsdata og om videre anvendelse af dataene. Formålet med disse artikler skulle være at sikre, at dataene kun anvendes til de formål, der er nævnt i artikel 3, stk. 2, at myndighederne varetager de modtagne datas kvalitet, hemmelighed og sikkerhed, og at dataene slettes, når de ikke længere skal bruges til forebyggelse, efterforskning, afsløring

og strafforfølgning af de specifikke lovovertrædelser. Desuden bør det fastsættes, at adgang i bestemte tilfælde skal være underlagt domstolskontrol i medlemsstaterne.

57. For det femte indeholder forslaget ikke yderligere garantier for databeskyttelse. I betragtningerne henvises der blot til garantier i den gældende lovgivning, særlig direktiv 95/46/EF og direktiv 2002/58/EF. Den tilsynsførende finder denne begrænsede tilgang til databeskyttelse forkert i betragtning af, at (yderligere) garantier er af særlig vigtighed (se afsnit II i denne udtalelse).

58. Derfor anbefaler den tilsynsførende, at der medtages et stykke om databeskyttelse. I dette stykke kunne ovenstående anbefalinger vedrørende artikel 3, stk. 2, indsættes sammen med andre bestemmelser om databeskyttelse såsom bestemmelser vedrørende den registreredes udøvelse af sine rettigheder (se afsnit II i denne udtalelse), datakvalitet og -sikkerhed og trafik- og lokaliseringsdata vedrørende personer, der ikke er mistænkt for lovovertrædelser.

Artikel 4: Kategorier af data, der skal opbevares

59. Generelt er den tilsynsførende godt tilfreds med artiklen og bilaget på grund af

— den valgte lovgivningsteknik med funktionelle beskrivelser i selve direktivteksten og tekniske detaljer i bilaget. Den er fleksibel nok til at kunne følge den teknologiske udvikling, og den giver borgerne retssikkerhed

— sondringen mellem data om telekommunikation og internetdata, selv om sondringen teknologisk set bliver mindre vigtig. Fra et databeskyttelsessynspunkt er sondringen imidlertid vigtig, da grænsen mellem indholdsdata og trafikdata på internettet er flydende (se f. eks. anerkendelsen i direktivets artikel 2, stk. 1, af, at oplysninger, der konsulteres på internettet, er indholdsdata).

— harmoniseringsniveauet: Forslaget tager sigte på et højt harmoniseringsniveau med en udtømmende liste over kategorier af data, der skal opbevares (i modsætning til udkastet til rammeafgørelse, der indeholder en minimumsliste med en bred margen for medlemsstaterne til at tilføje data). Fra et databeskyttelsessynspunkt er fuld harmonisering afgørende (se afsnit IV).

60. Den tilsynsførende anbefaler følgende ændringer:

— Artikel 4, stk. 2, bør indeholde mere præcise kriterier for at sikre, at indholdsdata ikke medtages. Følgende punktum bør tilføjes: »Bilaget må ikke omfatte data, der afslører en kommunikations indhold.«

— Artikel 5 åbner mulighed for revision af bilaget ved hjælp af et kommissionsdirektiv (»komitologi«). Den tilsynsførende tilråder, at revisioner af bilaget med en væsentlig indvirkning på databeskyttelsen helst skal ske i form af et direktiv efter den fælles beslutningsprocedure. ([1])

Artikel 7: Opbevaringsperioder

61. Den tilsynsførende ser med tilfredshed på, at opbevaringsperioderne i forslaget er betydeligt kortere end perioderne i udkastet til rammeafgørelse.

— Under henvisning til de betænkeligheder, der er givet udtryk for i denne udtalelse, med hensyn til, om det er nødvendigt at opbevare trafikdata i op til et år, afspejler perioden på et år retshåndhævelsespraksis, *som den er angivet* med de tal, som Kommissionen og Rådets formandskab har fremlagt.

— Disse tal viser også, at opbevaring af data i længere perioder kun i få tilfælde afspejler retshåndhævelsespraksis.

— En kortere periode på et halvt år for data vedrørende elektronisk kommunikation, der udelukkende eller hovedsagelig finder sted med brug af internetprotokollen, er vigtig ud fra et databeskyttelsessynspunkt, da opbevaring af resultater af internet-kommunikation medfører meget store databaser (disse data opbevares som regel ikke med henblik på debitering), grænsen mellem disse data og indholdsdata er flydende, og opbevaring i over et halvt år ikke afspejler retshåndhævelsespraksis.

62. Det bør fremgå klart af teksten,

— at opbevaringsperioderne på henholdsvis et halvt år og et år er maksimumsperioder

([1]) Se også den tilsynsførendes udtalelse af 23. marts 2005 om forslaget til Europa-Parlamentets og Rådets forordning om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (punkt 3.12).

— at dataene slettes, når opbevaringsperioden udløber. Det bør også fremgå klart, hvordan dataene skal slettes. Den tilsynsførende mener, at en udbyder skal slette dataene elektronisk mindst en gang om dagen.

Artikel 8: Lagringskrav for opbevarede data

63. Denne artikel er nært knyttet til artikel 3, stk. 2, og indeholder en vigtig bestemmelse, der kan sikre, at adgang i bestemte tilfælde kan begrænses til de data, der specifikt er behov for. Artikel 8 og artikel 3, stk. 2, forudsætter, at udbyderne sender de nødvendige data til myndighederne, og at disse ikke har direkte adgang til databaserne. Den tilsynsførende anbefaler, at denne forudsætning angives eksplicit i teksten.

64. Bestemmelsen bør gøres mere specifik ved at angive,

— at udbyderne sender de nødvendige data til myndighederne (se punkt 63)

— at udbyderne skal installere den nødvendige tekniske arkitektur, bl.a. søgemaskiner, for at lette en målrettet adgang til de specificerede data

— at udbyderne skal sikre, at kun deres medarbejdere med særlige tekniske beføjelser har adgang til databaserne af tekniske grunde, og at disse medarbejdere er klar over dataenes følsomme karakter og arbejder under strenge interne regler om tavshedspligt

— at dataene ikke alene skal fremsendes uden unødige forsinkelser, men også uden at afsløre andre trafik- og lokaliseringsdata end de data, der er nødvendige i forbindelse med anmodningen.

Artikel 9: Statistikker

65. Udbydernes pligt til at fremlægge statistikker en gang om året hjælper EF-institutionerne med at overvåge, om forslaget gennemføres og anvendes effektivt. Der er behov for tilstrækkelige oplysninger.

66. Den tilsynsførende mener, at denne pligt er en udmøntning af princippet om åbenhed. Den europæiske borger har ret til at vide, hvor effektiv dataopbevaringen er. Derfor bør udbyderen desuden have pligt til at føre logføringslister og til at foretage systematisk (egen-)kontrol, således at de nationale databeskyttelsesmyndigheder kan kontrollere databeskyttelsesreglernes anvendelse i praksis [1]. Forslaget bør ændres i den retning.

Artikel 10: Udgifter

67. Som nævnt i afsnit II er der en direkte forbindelse mellem tilstrækkelige sikkerhedsforanstaltninger og udgifterne hertil, med andre ord mellem sikkerhed og udgifter. Den tilsynsførende betragter derfor artikel 10 — der indeholder bestemmelser om godtgørelse af dokumenterede ekstraudgifter — som en vigtig bestemmelse, der kunne virke som et incitament for udbyderne til at investere i den tekniske infrastruktur.

68. Ifølge beregningerne i den konsekvensanalyse, som Kommissionen har forelagt for den tilsynsførende, er udgifterne til dataopbevaring betydelige. For en stor net- og tjenesteudbyder ville udgifterne være på over 150 mio. EUR for en opbevaringsperiode på et år med årlige driftsudgifter på omkring 50 mio. EUR. [2] Der foreligger dog ingen tal for udgifterne til yderligere sikkerhedsforanstaltninger såsom dyre søgemaskiner (se bemærkningen til artikel 6) eller for de (anslåede) finansielle følger af fuld godtgørelse af udbydernes ekstraudgifter.

69. Den tilsynsførende mener, at der er brug for mere præcise tal for at kunne vurdere forslaget i dets fulde omfang. Han foreslår, at forslagets finansielle følger angives nærmere i begrundelsen.

70. Med hensyn til bestemmelsen i selve artikel 10 bør forbindelsen mellem tilstrækkelige sikkerhedsforanstaltninger og udgifterne fremgå klart af bestemmelsens tekst. Desuden bør forslaget indeholde minimumsstandarder for de sikkerhedsforanstaltninger, som udbyderne skal træffe, for at de kan få godtgjort udgifterne af en medlemsstat. Den tilsynsførende mener, at fastsættelsen af disse standarder ikke fuldstændigt

---

[1] Se også den tilsynsførendes udtalelse af 23. marts 2005 om forslaget til Europa-Parlamentets og Rådets forordning om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (punkt 3.9).

[2] Kommissionen henviser til tal fra ETNO (Association of European Telecommunications Networks Operators) og til en betænkning fra MEP Alexander Nuno Alvaro om udkastet til rammeafgørelse.

kan overlades til medlemsstaterne. Det kunne skade det harmoniseringsniveau, som direktivet tilsigter. Desuden bør der tages hensyn til, at medlemsstaterne bærer de økonomiske følger af godtgørelsen.

Artikel 11: Ændring af direktiv 2002/58/EF

71. Forbindelsen til artikel 15, stk. 1, i direktiv 2002/58/EF bør fremgå klarere, da forslaget fratager denne bestemmelse en stor del af dens indhold. Henvisningerne i artikel 15, stk. 1, i direktiv 2002/58/EF til artikel 6 og 9 (i samme direktiv) bør udgå eller i hvert fald ændres, således at det er tydeligt, at medlemsstaterne ikke længere er kompetente til at vedtage anden lovgivning vedrørende lovovertrædelser end omhandlet i forslaget. Tvetydighed med hensyn til, hvilken kompetence de stadig har — f.eks. med hensyn til opbevaring af data i forbindelse med »ikke-grov« kriminalitet — skal fjernes.

Artikel 12: Evaluering

72. Den tilsynsførende er godt tilfreds med, at forslaget indeholder en artikel om, at direktivet skal evalueres inden tre år efter dets ikrafttræden. En evaluering er så meget vigtigere, som der kan være tvivl om forslagets nødvendighed og dets proportionalitet.

73. Derfor tilråder den tilsynsførende, at der fastsættes en endnu strengere pligt, der indeholder følgende elementer:

— Evalueringen skal omfatte en vurdering af, om direktivet gennemføres effektivt fra et retshåndhævelsessynspunkt, og en vurdering af følgerne for den registreredes grundlæggende rettigheder. Kommissionen skal medtage alle fakta, der kan påvirke evalueringen.

— Evalueringen skal foretages regelmæssigt (mindst hvert andet år).

— Kommissionen skal have pligt til i givet fald at forelægge ændringer til forslaget (som i henhold til artikel 18 i direktiv 2002/58/EF).

VI. Konklusioner

Forudsætninger

74. Den tilsynsførende finder det afgørende, at forslaget respekterer de grundlæggende rettigheder. En lovgivning, der ville skade den beskyttelse, som er sikret ved fællesskabsretten og mere specifikt ved Domstolens og Den Europæiske Menneskerettighedsdomstols retspraksis, er ikke alene uacceptabel, men også ulovlig.

75. Behovet for og proportionaliteten i pligten til at opbevare — samtlige — data skal godtgøres.

76. Med hensyn til nødvendigheden: Den tilsynsførende erkender, at forholdene ændrer sig, men er endnu ikke overbevist om, at det er nødvendigt at opbevare trafik- og lokaliseringsdata med henblik på retshåndhævelse som fastsat i forslaget.

77. Den tilsynsførende tilkendegiver ikke desto mindre sin mening om forslagets proportionalitet i denne udtalelse. Det betyder for det første, at opbevaring af trafik- og lokaliseringsdata ikke i sig selv er et tilstrækkeligt eller effektivt tiltag. Der er behov for yderligere foranstaltninger for at sikre, at myndighederne har en målrettet og hurtig adgang til de data, de har brug for i en bestemt sag. For det andet skal forslaget

— begrænse opbevaringsperioderne. Perioderne skal afspejle de påviste behov for retshåndhævelse

— begrænse antallet af data, der skal lagres. Dette antal skal afspejle de påviste behov for retshåndhævelse, og det skal sikres, at der ikke er adgang til indholdsdata

— indeholde tilstrækkelige sikkerhedsforanstaltninger.

Generel vurdering

78. Den tilsynsførende understreger betydningen af, at forslagets tekst tager sigte på fuld harmonisering af forslagets hovedelementer, især de typer data, der skal opbevares, opbevaringsperioderne samt (formålene med) adgangen til og videre anvendelse af dataene.

79. Nogle punkter skal klarlægges nærmere, f.eks. for at sikre, at data slettes på en tilstrækkelig måde, når opbevaringsperioden udløber, og for effektivt at forebygge forskellige grupper af interessenters adgang og anvendelse.

80. Den tilsynsførende finder følgende punkter afgørende for, at forslaget kan accepteres fra et databeskyttelsessynspunkt:

— I forslaget tilføjes der specifikke bestemmelser om de kompetente myndigheders adgang til og videre anvendelse af dataene som et væsentligt element, der er uløseligt forbundet med emnet.

— I forslaget tilføjes der yderligere garantier for databeskyttelse (i modsætning til blot at henvise til garantier i den gældende lovgivning, særlig direktiv 95/46/EF og direktiv 2002/58/EF), bl.a. for at sikre, at de registrerede kan udøve deres rettigheder.

— I forslaget tilføjes der yderligere incitamenter for udbyderne til at investere i den tekniske infrastruktur, bl.a. økonomiske incitamenter. Denne infrastruktur kan kun blive tilstrækkelig, hvis der findes effektive søgemaskiner.

Anbefalede ændringer af forslaget

81. Artikel 3, stk. 2:

— Der tilføjes en bestemmelse for at sikre, at andre end de kompetente myndigheder ikke har adgang til dataene. Denne bestemmelse kunne affattes således: »Der gives kun mulighed for adgang til og/eller behandling af dataene til det formål, der er nævnt i artikel 3, stk. 2« eller »Udbyderne skal effektivt sikre, at kun de kompetente myndigheder får adgang«.

— Det fastsættes, at data kun kan udleveres, hvis det er nødvendigt i forbindelse med en specifik lovovertrædelse.

— Udlevering skal kun ske i forbindelse med *visse former for* grov kriminalitet.

— Der tilføjes en eller flere artikler i forslaget om de kompetente myndigheders adgang til trafik- og lokaliseringsdata og om videre anvendelse af dataene og af en bestemmelse om, at adgang i bestemte tilfælde skal være underlagt domstolskontrol i medlemsstaterne.

— Der medtages et stykke om databeskyttelse.

82. Artikel 4 og 5:

— Følgende punktum tilføjes i artikel 4, stk. 2: »Bilaget må ikke omfatte data, der afslører en kommunikations indhold.«

— Det angives, at revisioner af bilaget med en væsentlig indvirkning på databeskyttelsen helst skal ske i form af et direktiv efter den fælles beslutningsprocedure.

83. Artikel 7: Det bør fremgå klart af teksten,

— at opbevaringsperioderne på et halvt år og et år er maksimumsperioder

— at dataene slettes, når opbevaringsperioden udløber. Det bør også fremgå klart, hvordan dataene skal slettes, nemlig at en udbyder skal slette dem elektronisk mindst en gang om dagen.

84. Artikel 8: Det bør fremgå klart af teksten,

— at udbyderne sender de nødvendige data til myndighederne

— at udbyderne skal installere den nødvendige tekniske arkitektur, bl.a. søgemaskiner, for at lette en målrettet adgang til de specificerede data

— at udbyderne skal sikre, at kun deres medarbejdere med særlige tekniske beføjelser har adgang til databaserne af tekniske grunde, og at disse medarbejdere er klar over dataenes følsomme karakter og arbejder under strenge interne regler om tavshedspligt

— at dataene ikke alene skal fremsendes uden unødige forsinkelser, men også uden at afsløre andre trafik- og lokaliseringsdata end de data, der er nødvendige i forbindelse med anmodningen.

85. Artikel 9:

— Der tilføjes en bestemmelse om, at udbyderen har pligt til at føre logføringslister og til at foretage systematisk (egen-)kontrol, således at de nationale databeskyttelsesmyndigheder kan kontrollere databeskyttelsesreglernes anvendelse i praksis.

86. Artikel 10:

— Forbindelsen mellem tilstrækkelige sikkerhedsforanstaltninger og udgifterne bør fremgå klart af bestemmelsen.

— Der fastsættes minimumsstandarder for de sikkerhedsforanstaltninger, som udbyderne skal træffe, for at de kan få godtgjort udgifterne af en medlemsstat.

— Forslagets økonomiske følger skal angives nærmere i begrundelsen.

87. Artikel 11:

— Artikel 15, stk. 1, i direktiv 2002/58/EF ændres, således at henvisningerne til artikel 6 og 9 (i samme direktiv) udgår eller i hvert fald ændres, således at det er tydeligt, at medlemsstaterne ikke længere er kompetente til at vedtage anden lovgivning vedrørende lovovertrædelser end omhandlet i forslaget.

88. Artikel 12: Bestemmelsen om evaluering ændres således:

— Evalueringen skal omfatte en vurdering af, om direktivet gennemføres effektivt.

— Evalueringen skal foretages regelmæssigt (mindst hvert andet år).

— Kommissionen skal have pligt til at forelægge ændringer til forslaget, når det er hensigtsmæssigt (som i artikel 18 i direktiv 2002/58/EF).

Udfærdiget i Bruxelles den 26. september 2005.

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse