



EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 21.9.2005
KOM(2005) 438 slutlig

2005/0182 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om lagring av uppgifter som behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster och om ändring av direktiv 2002/58/EG

(framlagt av kommissionen)

SEC(2005) 1131}

MOTIVERING

1. BAKGRUND

- **Syftet med förslaget**

Medborgarna använder allt oftare elektroniska tjänster och nät i sitt dagliga liv. Detta genererar s.k. trafikuppgifter eller lokaliseringssuppgifter, t.ex. om vem som ringt ett samtal, vilket nummer som ringts upp samt tidpunkt och samtalets längd. När sådana trafikuppgifter kombineras med uppgifter som gör det möjligt att identifiera den som abonnerar på eller använder en tjänst blir de viktiga i samband med brottsbekämpning och säkerhet, t.ex. för att förebygga, utreda, avslöja och åtala allvarliga brott som terrorism och organiserad brottslighet.

Allteftersom affärsmodeller och tjänsteutbud förändras, t.ex. genom ökad användning av enhetstaxor och förbetalda eller gratis kommunikationstjänster kan trafikuppgifter inte alltid lagras av operatörerna i samma utsträckning som skett tidigare, beroende på vilka tjänster de erbjuder. Detta är också fallet med nyheter som IP-telefoni eller fasta taxor för fast telefoni. Under sådana omständigheter behöver operatörerna inte längre lagra trafikuppgifter för att kunna fakturera kunderna. Om trafikuppgifter inte lagras för t.ex. fakturerings syfte är de inte tillgängliga för myndigheter i de fall där det finns ett legitimt behov av sådana uppgifter. Denna utveckling gör det med andra ord mycket svårare för myndigheterna att uppfylla sin skyldighet vad gäller att förebygga och bekämpa organiserad brottslighet och terrorism, och gör det enklare för kriminella att kommunicera med varandra utan att behöva oroa sig för att kommunikationsuppgifterna skall kunna användas för att hindra deras verksamhet.

Det är därför angeläget att snarast anta enhetliga EU-bestämmelser på detta område. En del medlemsstater har antagit eller planerar att anta nationella åtgärder för att tvinga operatörerna att lagra vissa typer av uppgifter så att dessa kan användas i sådana fall som beskrivs ovan. Skillnader i rättsliga, reglerande och tekniska bestämmelser i medlemsstaterna avseende lagring av trafikuppgifter utgör hinder för den inre marknaden för elektronisk kommunikation, eftersom tjänsteleverantörer ställs inför mycket olika krav avseende typen av uppgifter som skall lagras och villkoren för detta. Bestämmelserna på detta område bör därför harmoniseras ytterligare i enlighet med artikel 14 i EG-fördraget.

- **Allmän bakgrund**

Att det är nödvändigt med bestämmelser på EU-nivå för att säkerställa att trafikuppgifter finns tillgängliga i samtliga 25 medlemsstater för terrorismbekämpning bekräftades av Europeiska rådet i uttalandet om terrorismbekämpning av den 25 mars 2004. Efter bombattentaten i Madrid fick rådet i uppdrag av Europeiska att undersöka ”förslag för att fastställa regler för lagring av trafikuppgifter från kommunikation hos tjänsteoperatörer” med avsikten att sådana regler skulle antas under 2005. Att antagandet av ett lämpligt rättsligt instrument på detta område är en prioritet bekräftades nyligen i slutsatserna från Europeiska rådets möte den 16–17 juni samt vid det särskilda mötet med rådet (rättsliga och inrikes frågor) den 13 juli 2005 efter terroristattacker i London.

- **Befintliga bestämmelser på området**

Genom artiklarna 6 och 9 i direktiv 2002/58/EG om integritet och elektronisk kommunikation harmoniseras de bestämmelser om skydd av personuppgifter som gäller för bearbetning av trafik- och lokaliseringssuppgifter som genererats i samband med användningen av elektroniska kommunikationstjänster. Sådana uppgifter måste utplånas eller avidentifieras när de inte längre används för överföring, med undantag av uppgifter som krävs för abonnentfakturerings eller betalning av samtrafikuppgifter. Förutsatt att medgivande ges kan vissa uppgifter också användas för marknadsföring eller för att tillhandahålla mervärdestjänster. I artikel 15.1 föreskrivs det att medlemsstaterna får begränsa tillämpningen av bl.a. artiklarna 5, 6 och 9 om begränsningarna är nödvändiga, lämpliga och proportionella i ett demokratiskt samhälle för att skydda den nationella säkerheten, försvaret samt den allmänna säkerheten och för att förebygga, utreda, avslöja och åtala brott.

- **Förenlighet med Europeiska unionens politik och mål på andra områden**

Förslaget är i linje med gemenskapslagstiftningen och stadgan om de grundläggande rättigheterna. Även om det är uppenbart att förslaget till direktiv kommer att påverka medborgarnas rätt till skydd av privatlivet enligt artikel 7 i stadgan, liksom rättigheten till skydd av personuppgifter enligt artikel 8, är detta berättigat enligt stadgans artikel 52. De inskränkningar av dessa rättigheter som förslaget innebär är proportionella och nödvändiga om det gemensamt erkända målet att förebygga och bekämpa brottslighet och terrorism skall kunna uppnås.

Förslagets inflytande på medborgarnas privatliv begränsas dessutom: för det första genom att det klart fastställs för vilka ändamål de lagrade uppgifterna får användas, för det andra genom att man begränsar den typ av uppgifter som får lagras, och för det tredje genom att man begränsar den tid uppgifterna lagras. Ytterligare en viktig säkerhetsmekanism är att direktivet inte är tillämpligt på själva kommunikationsinnehållet, eftersom detta innebär avlyssning av telekommunikation, något som faller utanför direktivets tillämpningsområde.

Behandlingen av de personuppgifter som lagras av tjänste- och nätleverantörer enligt direktivets bestämmelser omfattas av de allmänna och särskilda bestämmelser om skydd av personuppgifter som fastställts genom direktiven 95/46/EG och 2002/58/EG, vilket innebär att det i praktiken inte behövs några ytterligare bestämmelser om allmänna principer för skydd av personuppgifter och datasäkerhet. Detta innebär också att behandlingen av sådana uppgifter står under tillsyn av medlemsstaternas dataskyddsmyndigheter.

2. SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSPANALYS

• Samråd med berörda parter

Metoder, målsektorer och deltagarnas allmänna profil

Frågan om lagring av trafikuppgifter har, sedan Cybercrime Forums möten under 2001, varit föremål för samråd med företrädare för brottsbekämpande myndigheter, kommunikationssektorn och dataskyddsexperter.

Den 14 juni 2004 organiserade det europeiska forumet för förebyggande av organiserad brottslighet ett rundabordsmöte där företrädare för brottsbekämpande myndigheter, näringslivet och dataskyddsorganisationer deltog. Som del av förberedelserna inför en öppen workshop i frågan som hölls den 21 september 2004, presenterade GD INFSO och GD JLS den 30 juli 2004 ett gemensamt samrådsdokument om lagring av trafikuppgifter. Det inkom bidrag och reaktioner från deltagarna, särskilt från näringslivet och organisationer för medborgerliga rättigheter, på dokumentet. Vid den öppna workshop som hölls den 21 september fick kommissionen ytterligare kommentarer.

Som del av arbetet med att förbereda förslaget har kommissionen också tagit del av den breda offentliga debatten i frågan, inklusive de överläggningar som hållits i Europaparlamentet.

Sammanfattning av svaren och av hur de har beaktats

Vid samrådet bekräftades att brottsbekämpande myndigheter behöver trafikuppgifter för att förebygga och bekämpa brottslighet och terrorism. Dessa myndigheter ansåg att lagringstiden bör vara så lång som krävs och omfatta så mycket uppgifter som möjligt för att vara till nytta för dem. Särskilt i omfattande utredningar av allvarliga brott, som det kan ta flera år att slutföra, krävs ofta tillgång till äldre trafikuppgifter. Det gavs flera exempel på fall där sådana uppgifter hade varit avgörande för en brottsutredning, och det gällde särskilt brott som bombattentat och mord.

Företrädare för representativa europeiska organisationer från telekom- och Internetbranschen, liksom enskilda företag med verksamhet inom elektronisk kommunikation, framhöll att de är beredda att samarbeta med brottsbekämpande myndigheter, och även har gjort det, men att skulle långa lagringstider skulle innebära avsevärda kostnader och att det vore tillräckligt att säkra uppgifter. De argumenterade för att lagringstiden inte borde vara mer än sex månader eftersom de brottsbekämpande myndigheterna sällan begär uppgifter som är äldre än så. De efterlyste också mekanismer för att kompensera dem för merkostnaderna.

Företrädare för dataskyddsmyndigheter och organisationer för mänskliga rättigheter menade att lagring av uppgifter är ett intrång i medborgarnas privatliv, och att lagringstiden därför bör vara så kort som möjligt. De ifrågasatte om lagringstider på mer än sex månader kan anses vara proportionerligt. Likaså uttryckte de oro för syftet med att lagra uppgifter, som de ansåg borde specificeras tydligt.

I det nuvarande förslaget har dessa synpunkter beaktats, och förslaget grundas på den bifogade konsekvensanalysen. Lagringstiden på ett år för trafikuppgifter för mobil och fast telefoni och sex månader för Internetanvändning täcker de flesta behov som brottsbekämpande myndigheter har, samtidigt som därmed sammanhängande kostnader för industrin minskas och intrånget i medborgarnas privatliv begränsas. En lagringstid på sex månader för alla typer av uppgifter skulle ha varit för kort. Visserligen gäller de flesta förfrågningarna från brottsbekämpande myndigheter uppgifter som inte är äldre än sex månader, men i de fall äldre uppgifter behövs gäller de ofta mer allvarliga brott som terrorism, organiserad brottslighet och mord.

- **Extern experthjälp**

Någon extern experthjälp har inte behövts.

- **Konsekvensanalys**

Olika alternativ har beaktats. 2002 uppmanade rådet till dialog på nationell nivå och EU-nivå för att hitta lösningar på frågan om lagring av trafikuppgifter som fyller dels behovet av effektiva verktyg för att förebygga, avslöja, utreda och åtala brott, men också av att skydda privatpersoners grundläggande fri- och rättigheter, särskilt rätten till skydd av privatlivet, av personuppgifter och av brev- och telehemligheter. Det offentliga samrådet och debatten i frågan, bl.a. i Europaparlamentet, har varit omfattande. Man har dock inte kommit överens om några gemensamma lösningar.

Att inte ta något initiativ till lagring av uppgifter skulle innebära att den nuvarande situationen med splittrade bestämmelser kvarstår. Alternativet icke-bindande regler har förkastats eftersom de skulle innebära otillfredsställande rättssäkerhet. Likaså har initiativ inom tredje pelaren förkastats eftersom det inte skulle ha överensstämt med befintlig gemenskapsrätt. Europeiska rådet efterlyste också lagstiftning i sitt uttalande om kampen mot terrorism.

Ett förslag till direktiv däremot ger den grad av harmonisering som behövs på den inre marknaden. Jämfört med en förordning lämnar den visst manövreringsutrymme till medlemsstaterna vid genomförandet av bestämmelser på detta känsliga område. En förordning skulle ha varit alltför strikt, särskilt med tanke på de olika tekniska arkitekturer som operatörerna i olika länder använder. Direktivet lämnar tillräckligt med svängrum för medlemsstaterna att införa nationella begränsningar. Den situation som råder idag är hursomhelst inte hållbar längre eftersom de varierande nationella bestämmelserna på området leder till hinder för det fria tillhandahållandet av tjänster. Valet av rättsligt instrument, och artikel 95 i EG-fördraget som rättslig grund, rekommenderades också i den rättsliga analysen i kommissionens arbetsdokument SEK (2005) 420 av den 22 mars 2005. Kommissionen har gjort en konsekvensanalys som finns på http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3. RÄTTSLIGA ASPEKTER

- **Sammanfattning av den föreslagna åtgärden**

Förslaget till direktiv är avsett att harmonisera den skyldighet som leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät har att lagra vissa trafikuppgifter, så att behöriga myndigheter i medlemsstaterna kan få tillgång till dessa för att förebygga, utreda, avslöja och åtala allvarliga brott som terrorism och organiserad brottslighet.

- **Rättslig grund**

Artikel 95 i EG-fördraget.

- **Subsidiaritetsprincipen**

Subsidiaritetsprincipen är tillämplig eftersom förslaget inte uteslutande faller inom gemenskapens behörighetsområde.

Medlemsstaterna kan av följande skäl inte i tillräcklig utsträckning själva uppnå förslagets mål:

Harmonisering av lagringstiden för lagring av trafikuppgifter är inget som medlemsstaterna själva kan åstadkomma. Endast insatser på EU-nivå, vilket också efterlystes av Europeiska rådet, kan säkerställa att trafikuppgifter lagras inom hela EU och kan göras tillgängliga för brottsbekämpande myndigheter.

Eftersom det till stor del beror på internationellt samarbete om brottsutredningar skall bli framgångsrika, och olika nationella val har negativ effekt på marknaden för elektroniska kommunikationer, är EU-täckande harmonisering av bestämmelser om lagring av trafikuppgifter den lämpligaste vägen att gå. Principen om kostnadsersättning gör det möjligt att skapa lika förutsättningar för leverantörer av elektroniska kommunikationstjänster på den inre marknaden.

Om gemenskapen vidtar åtgärder kan förslagets mål enklare uppnås:

EU-åtgärder kommer att göra det enklare att uppnå förslagets mål genom att det säkerställs att trafikuppgifter lagras på ett enhetligt sätt inom hela EU och kan göras tillgängliga för brottsbekämpande myndigheter på samma villkor i alla medlemsstater. Detta kommer också att innebära fördelar för kommunikationsindustrin, särskilt de företag som bedriver verksamhet i flera medlemsstater, eftersom deras teknik kan standardiseras.

De kvalitativa indikatorer som visar att målet kan uppnås bättre på EU-nivå är hur effektivt brottsbekämpande myndigheter kan förebygga och bekämpa brott och terrorism, särskilt när det gäller organiserad brottslighet och terrorism, som ofta är gränsöverskridande.

Genom att förslaget begränsas till att gälla skyldigheter för leverantörer av elektroniska kommunikationstjänster eller allmänna kommunikationsnät att lagra

uppgifter täcker det bara åtgärder som bäst genomförs på EU-nivå och där medlemsstaterna själva inte kan åstadkomma tillfredsställande resultat. Förslaget innebär att medlemsstaterna själva kan välja vilka myndigheter som skall få tillgång till de lagrade uppgifterna och på vilka villkor. Tillgång till och utbyte av information mellan berörda brottsbekämpande myndigheter är något som faller utanför EG-fördragets tillämpningsområde.

I detta sammanhang är det värt att nämna att kommissionen för närvarande håller på att utarbeta lagstiftningsförslag under EU-fördraget vad gäller principen om tillgång till information för brottsbekämpning och inrättandet av dataskyddsprinciper för den tredje pelaren. Vidare bör det påpekas att "lagrade uppgifter" enligt detta direktiv bara skall vara tillgängliga för brottsbekämpning. Leverantörer av elektroniska kommunikationstjänster skall alltså inte få tillgång till uppgifterna.

Förslaget är därför förenligt med subsidiaritetsprincipen.

- **Proportionalitetsprincipen**

Förslaget överensstämmer med proportionalitetsprincipen eftersom dess inverkan på medborgare och näringsliv har begränsats så långt det varit möjligt. Det bör upprepas att förslaget endast gäller trafikuppgifter som behandlas av leverantörer av elektroniska kommunikationstjänster. Innehållet i elektronisk kommunikation omfattas inte av direktivet.

Respekten för grundläggande fri- och rättigheter, särskilt rätten till liv, och den strikta begränsningen av förslagets inverkan på privatlivet, har varit den viktigaste drivkraften i arbetet med att hitta en lämplig balans mellan alla berörda intressen, såväl sociala, ekonomiska och säkerhetsmässiga som vad gäller skydd av privatlivet.

I detta förslag till direktiv har man därför beaktat proportionalitetsfrågan, främst vad gäller de lagringstider som föreslagits, åtskillnaden mellan telefon- och Internetuppgifter samt begränsningen av de typer av uppgifter som skall lagras och systemet för kostnadsersättning. Förslaget innebär särskilt en klar begränsning av de syften de lagrade uppgifterna får användas för. Dataskyddslagstiftningen kommer att gälla för de lagrade uppgifterna, medan inverkan på individens rättigheter och de ekonomiska aktörerna begränsas genom att det endast är vissa begränsade uppgifter som skall lagras. Genom att lagringstiden för trafikuppgifter som gäller Internetanvändning blir kortare än för trafikuppgifter från fast och mobil telefoni tar man hänsyn till praxis inom affärlivet, eftersom de uppgifter som skall lagras blir avsevärt färre.

Den ekonomiska och administrativa bördan för nationella regeringar, ekonomiska aktörer och medborgare har minimerats på flera sätt. För det första innebär direktivet en harmonisering, vilket innebär minskade kostnader för att efterleva direktivet för leverantörerna av elektroniska kommunikationstjänster och allmänna kommunikationsnät. För det andra har kostnaderna minimerats genom den begränsade lagringstiden och de typer av uppgifter som skall lagras. Med tanke på hur viktig åtgärden är när det gäller att förebygga och bekämpa brottslighet och terrorism anses de merkostnader som förslagets bestämmelser om kostnadsersättning innebär för medlemsstaterna vara proportionerliga (se konsekvensanalysen).

Det bör också betonas att direktivet inte utesluter möjligheten att medlemsstaterna begär särskilda åtgärder för lagring av uppgifter i de fall där en misstänkt eller kriminell organisation redan har identifierats eller i särskilda fall som terroristattacker.

- **Val av regleringsform**

Föreslagen regleringsform: direktiv.

Några andra instrument skulle inte vara lämpliga av följande skäl:

Frågan om vilken som är den korrekta rättsliga grunden för ett förslag om lagring av trafikuppgifter har nyligen tagits upp i ett arbetsdokument från kommissionen. Kort sagt är ståndpunkten i detta dokument att frågan om lagring av trafikuppgifter redan har behandlats i tidigare rättsliga instrument med första pelaren som rättslig grund, t.ex. direktiven 2002/58/EG och 95/46/EG som nämns ovan. Analysen fortsätter med att påpeka att det bara var på grund av att man inte kunde nå politisk överenskommelse om lagringstidens längd som frågan inte harmoniserades fullt ut i direktiv 2002/58/EG, och man drar slutsatsen att andra rättsliga instrument gällande lagring av trafikuppgifter som sådana (till skillnad från bestämmelser som styr brottsbekämpande myndigheters utbyte av och tillgång till sådana uppgifter) också måste ha den första pelaren som rättslig grund. Denna logik överensstämmer med artikel 47 i EU-fördraget, där förhållandet mellan EU-fördraget och EG-fördraget regleras och det föreskrivs att inga rättsliga instrument som antagits under EU-fördraget får påverka den lagstiftning som antagits under EG-fördraget.

4. **BUDGETKONSEKVENSER**

Förslaget påverkar inte gemenskapens budget.

5. **YTTERLIGARE UPPLYSNINGAR**

- **Översyn/ändring/tidsbegränsning**

Förslaget inbegriper en bestämmelse om översyn. Man planerar att inrätta en expertpanel om lagring av uppgifter för att bistå kommissionen i översynsarbetet. En sådan grupp skulle kunna bestå av tekniska experter på elektronisk kommunikation men också av företrädare för brottsbekämpande myndigheter och dataskyddsmyndigheter.

- **Jämförelsetabell**

Medlemsstaterna skall till kommissionen överlämna texterna till nationella bestämmelser för genomförande av direktivet, tillsammans med en jämförelsetabell mellan dessa bestämmelser och bestämmelserna i detta direktiv.

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om lagring av uppgifter som behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster och om ändring av direktiv 2002/58/EG

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT
DETTA DIREKTIV

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 95,

med beaktande av kommissionens förslag¹,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande²,

med beaktande av Regionkommitténs yttrande³,

i enlighet med förfarandet i artikel 251 i fördraget, och

av följande skäl:

- (1) Enligt Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter⁴ skall medlemsstaterna säkerställa fysiska personers fri- och rättigheter i samband med behandling av personuppgifter, särskilt deras rätt till privatliv, för att garantera det fria flödet av personuppgifter inom gemenskapen.
- (2) I Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation⁵ översattes de principer som fastställts i direktiv 95/46/EG till specifika regler för elektronisk kommunikation.
- (3) I artiklarna 5, 6 och 9 i direktiv 2002/58/EG fastställs de bestämmelser som gäller för den behandling som nät- och tjänsteleverantörer gör av trafik- och lokaliseringssuppgifter som genereras vid användning av elektroniska kommunikationstjänster. Sådana uppgifter måste raderas eller göras anonyma när de inte längre används för överföring, med undantag av uppgifter som krävs för

1 EUT C [...], [...], s. [...].

2 EUT C [...], [...], s. [...].

3 EUT C [...], [...], s. [...].

4 EGT L 281, 23.11.1995, s. 31.

5 EGT L 201, 30.7.2002, s. 37.

fakturering. Förutsatt att medgivande ges kan vissa uppgifter också användas för marknadsföring eller för att tillhandahålla mervärdestjänster.

- (4) I artikel 15.1 i direktiv 2002/58/EG fastställs de villkor på vilka medlemsstaterna får begränsa omfattningen av de rättigheter och skyldigheter som anges i artiklarna 5 och 6, artikel 8.1–8.4 och artikel 9 i detta direktiv. Sådana begränsningar måste anses vara nödvändiga, lämpliga och proportionella i ett demokratiskt samhälle för den allmänna ordningens skull, dvs. för att skydda nationell säkerhet (statens säkerhet), försvaret och allmän säkerhet eller för att förebygga, utreda, avslöja och åtala brott eller obehörig användning av ett elektroniskt kommunikationssystem.
- (5) Flera medlemsstater har antagit lagstiftning om leverantörers skyldighet att lagra trafikuppgifter för att kunna förebygga, utreda, avslöja och åtala brott.
- (6) Skillnader i rättsliga och tekniska bestämmelser i medlemsstaterna avseende lagring av trafikuppgifter i syfte att förebygga, utreda, avslöja och åtala brott utgör hinder för den inre marknaden för elektronisk kommunikation, eftersom tjänsteleverantörer ställs inför av mycket olika krav avseende typen av uppgifter som skall lagras liksom villkoren för lagring och lagringstiderna.
- (7) Rådet (rättsliga och inrikes frågor) ansåg i sina slutsatser av den 20 september 2001 att det måste säkerställas att brottsbekämpande myndigheter kan utreda brott där elektronisk kommunikation använts och att rättsliga åtgärder vidtas mot förövare av sådana brott, samtidigt som man upprätthåller en balans mellan skyddet av personuppgifter och de brottsbekämpande myndigheternas behov av tillgång till uppgifter för att kunna utreda brott.
- (8) I slutsatserna från rådet (rättsliga och inrikes frågor) av den 19 december 2002 understryks det att eftersom omfattningen av elektronisk kommunikation ökat avsevärt är uppgifter om sådan kommunikation särskilt viktiga och ett värdefullt verktyg när det gäller att förebygga, utreda, avslöja och åtala brott, särskilt organiserad brottslighet.
- (9) I Europeiska rådets uttalande om kampen mot terrorism av den 25 mars 2004 ges rådet i uppdrag att undersöka ”förslag för att fastställa regler för lagring av trafikuppgifter från kommunikation hos tjänsteoperatörer”.
- (10) I det uttalande som antogs vid rådets informella möte den 13 juli 2005 upprepades behovet av att så snart som möjligt anta åtgärder för lagring av trafikuppgifter från elektronisk kommunikation.
- (11) Med tanke på hur viktiga trafikuppgifter är för att kunna förebygga, utreda, avslöja och åtala allvarliga brott som terrorism och organiserad brottslighet, något som framkommit både genom forskning och genom medlemsstaternas praktiska erfarenheter, är det viktigt att säkerställa att uppgifter som behandlas av leverantörer av elektroniska kommunikationstjänster eller kommunikationsnät lagras under en viss tid.
- (12) De typer av uppgifter som skall lagras har valts för att åstadkomma balans mellan å ena sidan de fördelar lagring av uppgifter innebär för förebyggande, utredning, avslöjande och åtal av allvarliga brott och å andra sidan den grad av intrång i

privatlivet som lagring av uppgifter orsakar. Lagringstiderna på ett år respektive sex månader för Internetkommunikation är också de avsedda att beakta alla intressen.

- (13) Med tanke på att lagring av uppgifter ger upphov till omfattande kostnader för kommunikationsleverantörer, medan fördelarna med ökad säkerhet kommer hela samhället till del, är det lämpligt att medlemsstaterna ersätter de kostnader som leverantörerna kan visa att de ådragit sig för att kunna efterleva de skyldigheter de får genom direktivet.
- (14) Den teknik som används för elektronisk kommunikation utvecklas snabbt, och de behöriga myndigheternas krav kan därför komma att ändras. För att få råd i dessa frågor planerar kommissionen att inrätta en expertpanel med företrädare för brottsbekämpande myndigheter, sammanslutningar inom den elektroniska kommunikationsindustrin samt dataskyddsmyndigheter.
- (15) Direktiv 95/46/EG⁶ och direktiv 2002/58/EG⁷ är tillämpliga på uppgifter som lagras i enlighet med detta direktiv; i artikel 30.1 c i direktiv 95/46/EG föreskrivs att artikel 29-gruppen skall rådfrågas.
- (16) Det är nödvändigt att medlemsstaterna vidtar lagstiftande åtgärder som säkerställer att uppgifter som lagras i enlighet med detta direktiv bara är tillgängliga för behöriga nationella myndigheter i enlighet med nationell lagstiftning, och på ett sätt som gör att berörda personers grundläggande rättigheter respekteras. Sådana åtgärder kan särskilt gälla lämpliga villkor, begränsningar och säkerhetsmekanismer för att säkerställa att lagrade uppgifter tillhandahålls på ett sätt som överensstämmer med grundläggande rättigheter såsom de garanteras i Europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.
- (17) De åtgärder som är nödvändiga för att genomföra detta direktiv bör antas i enlighet med rådets beslut 1999/468/EG av den 28 juni 1999 om de förfaranden som skall tillämpas vid utövandet av kommissionens genomförandebefogenheter⁸.
- (18) Syftet med åtgärden, att harmonisera leverantörernas skyldighet att lagra vissa uppgifter och säkerställa att de är tillgängliga för förebyggande, utredning, avslöjande och åtal av allvarliga brott som terrorism och organiserad brottslighet, är på grund av åtgärdens omfattning och de konsekvenser den får inget medlemsstaterna själva kan uppnå i tillräcklig grad, utan något som bättre uppnås på gemenskapsnivå. Därför får gemenskapen vidta åtgärder i enlighet med subsidiaritetsprincipen och artikel 5 i fördraget. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.
- (19) Denna rättsakt respekterar de grundläggande rättigheterna och iakttar de principer som erkänns som allmänna gemenskapsrättsliga principer, bland annat i Europeiska unionens stadga om de grundläggande rättigheterna. Detta direktiv tillsammans med direktiv 2002/58/EG syftar särskilt att säkerställa fullständig respekt för de grundläggande rättigheterna med avseende på privatlivet och medborgarnas kommunikation samt skyddet av personuppgifter (artiklarna 7 och 8 i stadgan).

⁶ EGT L 281, 23.11.1995, s. 31.

⁷ EGT L 201, 30.7.2002, s. 37.

⁸ EGT L 184, 17.7.1999, s. 23.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte och tillämpningsområde

1. Syftet med detta direktiv är att harmonisera medlemsstaternas bestämmelser om de skyldigheter som leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät har att behandla och lagra vissa uppgifter så att uppgifterna är tillgängliga för förebyggande, utredning, avslöjande och åtal av allvarliga brott som terrorism och organiserad brottslighet.
2. Direktivet skall gälla trafik- och lokaliseringssuppgifter för såväl fysiska som juridiska personer, samt de uppgifter som är nödvändiga för att kunna identifiera abonnenten eller den registrerade användaren. Det skall inte vara tillämpligt på innehållet i elektronisk kommunikation, inklusive sådan information som användaren sökt med hjälp av ett elektroniskt kommunikationsnät.

Artikel 2

Definitioner

1. I detta direktiv skall definitionerna i direktiv 95/46/EG, direktiv 2002/21/EG⁹ samt direktiv 2002/58/EG gälla.
2. I detta direktiv avses med
 - a) *uppgifter*: trafik- och lokaliseringssuppgifter samt de uppgifter som behövs för att identifiera en abonnent eller användare,
 - b) *användare*: en fysisk eller juridisk person som använder en allmänt tillgänglig elektronisk kommunikationstjänst för privat eller affärsmässigt bruk, utan att nödvändigtvis ha abonnerat på denna tjänst.

Artikel 3

Skyldighet att lagra uppgifter

1. Genom avvikelser från artiklarna 5, 6 och 9 i direktiv 2002/58/EG skall medlemsstaterna anta åtgärder för att säkerställa lagring enligt bestämmelserna i detta direktiv av uppgifter som genereras eller behandlas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller offentliga kommunikationsnät inom deras territorium i samband med att de levererar kommunikationstjänster.
2. Medlemsstaterna skall anta åtgärder för att säkerställa att uppgifter som lagras i enlighet med detta direktiv endast görs tillgängliga för behöriga nationella myndigheter, i särskilda fall och i enlighet med nationell lagstiftning, i syfte att förebygga, utreda, avslöja och åtala allvarliga brott som terrorism och organiserad brottslighet.

⁹ EGT L 108, 24.4.2002, s. 33.

Artikel 4
Typer av uppgifter som skall lagras

Medlemsstaterna skall säkerställa att följande uppgifter lagras i enlighet med direktivet:

- (a) Uppgifter som är nödvändiga för att spåra och identifiera en kommunikationskälla.
- (b) Uppgifter som är nödvändiga för att spåra och identifiera slutmålet för en kommunikation.
- (c) Uppgifter som är nödvändiga för att spåra och identifiera datum, tidpunkt och varaktighet för en kommunikation.
- (d) Uppgifter som är nödvändiga för att identifiera typen av kommunikation.
- (e) Uppgifter som är nödvändiga för att identifiera den utrustning som använts för kommunikationen, eller den utrustning som tros ha använts.
- (f) Uppgifter som är nödvändiga för att identifiera var mobil kommunikationsutrustning är belägen.

De typer av uppgifter inom respektive kategori som skall lagras specificeras i bilagan.

Artikel 5
Översyn av bilagan

Bilagan skall regelbundet ses över i enlighet med förfarandet i artikel 6.2.

Artikel 6
Kommitté

1. Kommissionen skall biträdas av en kommitté som skall bestå av företrädare för medlemsstaterna och ha kommissionens företrädare som ordförande.
2. När det hänvisas till denna punkt skall artiklarna 5 och 7 i beslut 1999/468/EG tillämpas, med beaktande av bestämmelserna i artikel 8 i det beslutet.
3. Den tid som avses i artikel 5.6 i beslut 1999/468/EG skall vara tre månader.

Artikel 7
Lagringstider

Medlemsstaterna skall säkerställa att de kategorier uppgifter som avses i artikel 4 lagras under en period av ett år från det datum kommunikationen ägde rum, med undantag av uppgifter som gäller elektronisk kommunikation som skett helt eller delvis via Internet. Uppgifter som gäller Internetkommunikation skall lagras i 6 månader.

Artikel 8
Krav för lagring av uppgifter

Medlemsstaterna skall säkerställa att uppgifter lagras i enlighet med detta direktiv på ett sådant sätt att uppgifterna och annan nödvändig relaterad information utan dröjsmål kan ställas till de behöriga myndigheternas förfogande när de begär det.

Artikel 9
Statistik

Medlemsstaterna skall säkerställa att Europeiska kommissionen varje år får statistik om lagring av de uppgifter som behandlas i samband med allmänna elektroniska kommunikationstjänster. Denna statistik skall innefatta följande:

- De fall där uppgifter skickats till behöriga myndigheter i enlighet med nationell lagstiftning.
- Den tid som gått från det datum då uppgifterna lagrades och det datum då den behöriga myndigheten begärde uppgifterna.
- De fall där en begäran om uppgifter inte kunde tillgodoses.

Sådan statistik skall inte omfatta personuppgifter.

Artikel 10
Kostnader

Medlemsstaterna skall säkerställa att leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät ersätts för de kostnader de kan visa att de haft för att efterleva de skyldigheter de åläggs i och med detta direktiv.

Artikel 11
Ändring av direktiv 2002/58/EG

I artikel 15 i direktiv 2002/58/EG skall följande infogas som punkt 1a:

”1a. Punkt 1 skall inte gälla skyldigheter som gäller lagring av uppgifter för att kunna förebygga, utreda, avslöja och åtala allvarliga brott som terrorism och organiserad brottslighet och som följer av direktiv 2005/.../EG. * * EUT L ,”.

Artikel 12
Utvärdering

1. Inom tre år från det datum som avses i artikel 13.1 skall kommissionen till Europaparlamentet och rådet översända en utvärdering av tillämpningen av detta direktiv och dess inverkan på de ekonomiska aktörerna och konsumenterna, med beaktande av den statistik som översänts till kommissionen i enlighet med artikel 9, i

syfte att avgöra om det är nödvändigt att ändra direktivets bestämmelser, särskilt vad avser de lagringstider som föreskrivs i artikel 7.

2. För detta ändamål skall kommissionen utreda alla synpunkter som inkommer från medlemsstaterna eller den arbetsgrupp för skydd av enskilda med avseende på behandlingen av personuppgifter som inrättats genom artikel 29 i direktiv 95/46/EG.

Artikel 13
Införlivande

1. Medlemsstaterna skall sätta i kraft de lagar och andra författningar som är nödvändiga för att följa detta direktiv senast [15 månader efter det att direktivet antagits]. Medlemsstaterna skall till kommissionen överlämna texten till dessa bestämmelser samt en jämförelsetabell över bestämmelserna i detta direktiv och de nationella bestämmelser som antagits.

När en medlemsstat antar dessa bestämmelser skall de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen skall göras skall varje medlemsstat själv utfärda.

2. Medlemsstaterna skall till kommissionen överlämna texten till de centrala bestämmelser i nationell lagstiftning som de antar inom det område som omfattas av detta direktiv.

Artikel 14
Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 15
Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Bryssel den

På Europaparlamentets vägnar
Ordförande

På rådets vägnar
Ordförande

Bilaga

Uppgifter som skall lagras inom de kategorier som anges i artikel 4 i direktivet:

- a) Uppgifter som är nödvändiga för att spåra och identifiera en kommunikationskälla.
 - (1) Telefoni i fasta nät:
 - (a) Det anropande telefonnumret.
 - (b) Abonentens eller den registrerade användarens namn och adress.
 - (2) Mobil telefoni:
 - (a) Det anropande telefonnumret.
 - (b) Abonentens eller den registrerade användarens namn och adress.
 - (3) Internetåtkomst, Internetbaserad e-post och Internettelefoni:
 - (a) Den IP-adress (Internet Protocol), oavsett om den är dynamisk eller statisk, som en kommunikation tilldelats av Internetleverantören.
 - (b) Användar-id för källan till kommunikationen.
 - (c) Nodetikett eller telefonnummer som tilldelats kommunikationen i det allmänna telenätet.
 - (d) Namn och adress för den abonnent eller registrerade användare som IP-adressen, nodetiketten eller användaridentiteten tilldelades i samband med kommunikationen.
- b) Uppgifter som är nödvändiga för att spåra och identifiera slutmålet för en kommunikation.
 - (1) Telefoni i fasta nät:
 - (a) Det uppringda telefonnumret.
 - (b) Abonentens eller den registrerade användarens namn och adress.
 - (2) Mobil telefoni:
 - (a) Det uppringda telefonnumret.
 - (b) Abonentens eller den registrerade användarens namn och adress.
 - (3) Internetåtkomst, Internetbaserad e-post och Internettelefoni:
 - (a) Den avsedda mottagarens nodetikett eller användar-id.
 - (b) Namn och adress för den abonnent eller registrerade användare som är den avsedda mottagaren.

- c) Uppgifter som är nödvändiga för att spåra och identifiera datum, tidpunkt och varaktighet för en kommunikation.
- (1) Telefoni i fasta nät och mobil telefoni:
 - (a) Datum och tid då kommunikationen påbörjades och avslutades.
 - (2) Internetåtkomst, Internetbaserad e-post och Internettelefoni:
 - (a) Datum och tid för på- respektive avloggning inom en given tidszon.
- d) Uppgifter som är nödvändiga för att identifiera typen av kommunikation.
- (1) Telefoni i fasta nät:
 - (a) Den telefonitjänst som använts, t.ex. rösttelefoni, konferenssamtal, fax- och meddelandetjänster.
 - (2) Mobil telefoni:
 - (a) Den telefonitjänst som använts, t.ex. rösttelefoni, konferenssamtal, SMS, EMS eller multimediatjänster.
- e) Uppgifter som är nödvändiga för att identifiera den utrustning som använts för kommunikationen, eller den utrustning som tros ha använts.
- (1) Mobil telefoni:
 - (a) Den uppringande och den uppringda partens IMSI (International Mobile Subscriber Identity).
 - (b) Den uppringande och den uppringda partens IMEI (International Mobile Equipment Identity).
 - (2) Internetåtkomst, Internetbaserad e-post och Internettelefoni:
 - (a) Det uppringande telefonnumret för uppringda förbindelser.
 - (b) DSL (Digital Subscriber Line) eller annat id för kommunikationens avsändare.
 - (c) MAC (Media Access Control) eller annat maskin-id för kommunikationens avsändare.
- f) Uppgifter som är nödvändiga för att identifiera var mobil kommunikationsutrustning är belägen.
- (1) Cell-id för kommunikationens början och slut.
 - (2) Dataavbildning mellan cell-id:n och deras geografiska placering vid kommunikationens början och slut.