EUROPEISKA UNIONENS RÅD

Bryssel den 19 april 2011 (3.5)
(OR. en)

9324/11

DAPIX 38
TELECOM 47
COPEN 85

FÖLJENOT

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
mottagen den:	18 april 2011
till:	Pierre de BOISSIEU, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	KOM(2011) 225 slutlig
Ärende:	RAPPORT FRÅN KOMMISSIONEN TILL RÅDET OCH EUROPAPARLAMENTET – Utvärderingsrapport om direktiv 2006/24/EG

För delegationerna bifogas kommissionens dokument – KOM(2011) 225 slutlig.

Bilaga: KOM(2011) 225 slutlig

EUROPEISKA KOMMISSIONEN

Bryssel den 18.4.2011
KOM(2011) 225 slutlig

RAPPORT FRÅN KOMMISSIONEN TILL RÅDET OCH EUROPAPARLAMENTET

Utvärderingsrapport om direktiv 2006/24/EG

RAPPORT FRÅN KOMMISSIONEN TILL RÅDET OCH EUROPAPARLAMENTET

Utvärderingsrapport om direktiv 2006/24/EG

1. INLEDNING

Enligt direktiv 2006/24/EG[1] (nedan kallat *direktivet*) är medlemsstaterna skyldiga att kräva att leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät (nedan kallade *operatörer*) lagrar trafik- och lokaliseringsuppgifter under en period av 6 till 24 månader för att säkerställa att uppgifterna finns tillgängliga för att kunna utreda, avslöja och åtala grova brott.

I denna rapport från kommissionen utvärderas, i enlighet med artikel 14 i direktivet, dess tillämpning av medlemsstaterna och dess inverkan på de ekonomiska aktörerna och konsumenterna, med beaktande av den fortsatta utvecklingen av tekniken för elektronisk kommunikation och den statistik som översänts till kommissionen i syfte att avgöra om det är nödvändigt att ändra direktivets bestämmelser, särskilt vad avser uppgiftstäckning och lagringsperioder. I rapporten undersöks också direktivets inverkan på de grundläggande rättigheterna mot bakgrund av den allmänna kritik som riktats mot lagringen av uppgifter och om åtgärder behövs för att hantera problem kopplade till användningen av anonyma SIM-kort i brottsligt syfte[2].

Generellt visas i utvärderingen att lagringen av uppgifter är ett värdefullt redskap vid brottsbekämpningen och för straffrättssystemen i EU. Direktivets bidrag till harmoniseringen av lagringen av uppgifter har begränsats t.ex. vad gäller ändamålsbegränsning och lagringsperioder, men också när det gäller att ersätta de kostnader som uppstår för operatörerna, vilket ligger utanför dess tillämpningsområde. Med hänsyn till konsekvenserna och riskerna för den inre marknaden och respekten för rätten till integritet och skydd av personuppgifter bör EU genom gemensamma regler fortsätta att säkerställa att höga standarder tillämpas vid lagring, hämtning och användning av trafik- och lokaliseringsuppgifter. Mot bakgrund av dessa slutsatser har kommissionen för avsikt att föreslå ändringar av direktivet. Dessa förslag till ändringar läggs fram på grundval av en konsekvensbedömning.

2. BAKGRUND TILL UTVÄRDERINGEN

Denna utvärderingsrapport har utformats efter omfattande diskussioner med och uppgifter från medlemsstaterna, experter och berörda aktörer.

---

[1] Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG, EUT L 105, 13.4.2006, s. 54.

[2] Rådets slutsatser om kampen mot brottsligt missbruk och anonym användning av elektronisk kommunikation, rådets 2908:e möte (rättsliga och inrikes frågor) i Bryssel den 27–28 november 2008.

I maj 2009 höll kommissionen en konferens kallad *Towards the Evaluation of the Data Retention Directive* med deltagare från datatillsynsmyndigheter, den privata sektorn, det civila samhället och den akademiska världen. I september 2009 sände kommissionen ett frågeformulär till berörda aktörer från dessa grupper. Den tog emot ett sjuttiotal svar[3] på frågeformuläret. Kommissionen höll en andra konferens i december 2010 kallad *Taking on the Data Retention Directive*, i vilken liknande berörda aktörer deltog för att dela preliminära bedömningar av direktivet och diskutera framtida frågor på området.

Kommissionen träffade företrädare från var och en av medlemsstaterna och de länder som är anslutna till avtalet om europeiska ekonomiska samarbetsområdet från oktober 2009 till mars 2010 för att mer ingående diskutera frågeställningarna i frågeformuläret avseende direktivets tillämpning. Medlemsstaterna började tillämpa direktivet senare än väntat, särskilt när det gäller internetrelaterade uppgifter. Det försenade införlivandet innebar att bara nio av medlemsstaterna kunde förse kommissionen med statistik från endera 2008 eller 2009, enligt kraven i artikel 10 i direktivet, även om sammanlagt 19 medlemsstater lämnade viss statistik (se avsnitt 4.7). Kommissionen skrev till medlemsstaterna i juli 2010 och begärde ytterligare kvantitativa och kvalitativa uppgifter avseende behovet av att lagra uppgifter för att få resultat vid brottsbekämpning. Tio medlemsstater svarade med att ge närmare uppgifter från särskilda fall där uppgifterna hade visat sig vara nödvändiga[4].

Denna rapport bygger på de ståndpunkter som antagits av ”Plattformen för elektronisk lagring av uppgifter för utredning, avslöjande och åtal av grova brott”[5] sedan den inrättades 2008. Kommissionen har beaktat rapporterna från artikel 29-gruppen[6], särskilt rapporten om den andra brottsbekämpningsåtgärden, dvs. gruppens bedömning av medlemsstaternas efterlevnad av direktivets krav på uppgiftsskydd och datasäkerhet[7].

3. LAGRING AV UPPGIFTER INOM EUROPEISKA UNIONEN

3.1. Lagring av uppgifter i straffrättsligt syfte och brottsbekämpningssyfte

Tjänste- och nätleverantörer (nedan kallade *operatörer*) bearbetar, i sin verksamhet, personuppgifter för överföring av meddelanden, fakturering, samtrafikavgifter, marknadsföring och vissa andra mervärdestjänster. Bearbetningen inbegriper uppgifter som

---

3 Svaren har offentliggjorts på kommissionens webbplats: (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm).

4 Belgien, Tjeckien, Cypern, Litauen, Ungern, Nederländerna, Polen, Slovenien, Förenade kungariket. Sverige rapporterade också flera fall av särskilt grova brott där historiska trafikuppgifter, vilka fanns tillgängliga trots avsaknaden av skyldigheten att lagra uppgifter, var avgörande för de fällande domarna.

5 Expertgruppen inrättades genom kommissionens beslut 2008/324/EG, EUT L 111, 23.4.2008, s. 11. Kommissionen har regelbundet träffat expertgruppen. Ståndpunkterna finns på http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm.

6 Arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter inrättades genom artikel 29 i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, EUT L 281, 23.11.1995, s. 31.

7 Rapport 1/2010 om den andra gemensamma brottsbekämpande åtgärden: Leverantörer av telekommunikationstjänsters och internettjänsteleverantörers förenlighet med kraven i nationell lagstiftning om lagring av trafikuppgifter med rättslig grund i artiklarna 6 och 9 i direktiv 2002/58/EG och direktiv 2006/24/EG om ändring av direktiv 2002/58/EG (WP 172), 13.7.2010, (se http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm).

anger källa, destination, datum, tidpunkt, varaktighet och typ av kommunikation, samt användarnas kommunikationsutrustning och, om mobiltelefoner används, uppgifter om var utrustningen finns. Enligt direktiv 2002/58/EG om integritetsskydd inom sektorn för elektronisk kommunikation[8] ska de trafikuppgifter som genereras genom användningen av elektroniska kommunikationstjänster i princip utplånas eller avidentifieras när dessa uppgifter inte längre behövs för att överföra kommunikation. Ett undantag får göras, under förutsättning att den abonnent eller användare som uppgifterna gäller har samtyckt till detta, i den utsträckning och under den tidsperiod som är nödvändig för faktureringsändamål. Lokaliseringsuppgifter får bara bearbetas om de avidentifieras eller om de användare som uppgifterna gäller samtycker till detta, i den utsträckning och under den tidsperiod som är nödvändig för att leverera en mervärdestjänst.

Innan direktivet trädde i kraft begärde nationella myndigheter tillgång till dessa uppgifter från operatörerna (åtkomsten omfattades av särskilda villkor) för att t.ex. identifiera abonnenter som använde en IP-adress, analysera kommunikationsverksamhet och identifiera lokaliseringen av en mobiltelefon.

På EU-nivå hanterades lagring och användning av uppgifter för brottsbekämpningsändamål först i direktiv 97/66/EG om behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet. Direktiv 97/66/EG var det första som gav medlemsstaterna möjlighet att vid behov anta lagstiftningsåtgärder för skydd av allmän säkerhet, försvaret eller statens säkerhet (inbegripet statens ekonomiska välfärd när verksamheten rör statens säkerhet) och statlig verksamhet inom det straffrättsliga området[9].

Denna bestämmelse utvecklades i direktiv 2002/58/EG som gör det möjligt för medlemsstaterna att anta lagstiftningsåtgärder som utgör undantag från principen om konfidentialitet vid kommunikation, som under vissa omständigheter inbegriper lagring, åtkomst och användning av uppgifter i brottsbekämpningssyfte. I artikel 15.1 tillåts medlemsstaterna att begränsa dessa rättigheter och skyldigheter, också genom uppgiftslagring under en begränsad period när en sådan begränsning är nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret, allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt telekommunikationssystem.

Den roll lagringen av uppgifter spelar vad gäller straffrättssystemen och brottsbekämpningen diskuteras vidare i avsnitt 5.

3.2. Syftet med direktiv 2006/24/EG och dess rättsliga grund

Till följd av bestämmelserna i direktiv 97/66/EG och 2002/58/EG, vilka tillåter medlemsstaterna att anta lagstiftning om lagring av uppgifter, var operatörerna i vissa medlemsstater tvungna att köpa utrustning för lagring av uppgifter och anställa personal för

---

[8] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT L 201, 31.7.2002, s. 37.

[9] Artikel 14.1 i Europaparlamentets och rådets direktiv 97/66/EG av den 15 december 1997 om behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet, EGT L 24, 30.1.1998, s. 1.

att hämta uppgifter för de brottsbekämpande myndigheternas räkning, medan operatörer i andra medlemsstater inte gjorde detta, vilket ledde till snedvridningar på den inre marknaden. Utvecklingen av affärsmodeller och utbudet av tjänster, som ökad användning av enhetstaxor och förbetalda eller gratis kommunikationstjänster, innebar att operatörerna av faktureringsskäl gradvis upphörde med att lagra trafikuppgifter och lokaliseringsuppgifter och därmed minskade tillgången till dessa uppgifter för straffrättsliga syften och brottsbekämpningsändamål. Terroristattackerna i Madrid 2004 och London 2005 gjorde det än mer brådskande att på EU-nivå diskutera hur dessa frågor skulle hanteras.

Mot denna bakgrund föreskrevs i direktiv 2006/24/EG att medlemsstaterna skulle ålägga leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster och kommunikationsnät en skyldighet att lagra kommunikationsuppgifter för att utreda, avslöja och åtala grova brott såsom de definieras av varje medlemsstat i den nationella lagstiftningen, och att i EU harmonisera vissa därtill hörande frågeställningar.

Direktivet ändrade artikel 15.1 i direktiv 2002/58/EG genom att en punkt infördes som anger att artikel 15.1 inte är tillämplig på uppgifter som lagras enligt direktiv 2006/24/EG[10]. Därför kan medlemsstaterna (som anges i skäl 12 i direktivet) fortsätta att göra undantag från principen om konfidentialitet vid kommunikation. Direktiv 2002/58/EG reglerar bara lagringen av uppgifter för det mer begränsade ändamålet att utreda, upptäcka och åtala grov brottslighet.

Detta komplicerade rättsliga förhållande mellan direktiv 2006/24/EG och direktiv 2002/58/EG, tillsammans med avsaknaden av en definition i något av de två direktiven av begreppet *grovt brott* gör det svårt att urskilja dels de åtgärder som medlemsstaterna har vidtagit för att införliva den skyldighet att lagra uppgifter som anges i direktivet och dels den mer allmänna praxisen i medlemsstaterna att lagra uppgifter som tillåts enligt artikel 15.1 i direktiv 2002/58/EG[11]. Detta förhållande diskuteras närmare i avsnitt 4.

Direktivet grundar sig på artikel 95 i fördraget om upprättandet av Europeiska gemenskapen (som ersatts av artikel 114 i fördraget om Europeiska unionens funktionssätt) vad gäller den inre marknadens upprättande och funktion. Efter det att direktivet hade antagits ifrågasattes dess rättsliga grund av EU-domstolen med angivande av skälet att det primära målet var att utreda, avslöja och åtala grova brott. Domstolen framhöll att direktivet reglerade verksamhet som var oberoende av genomförandet av något som helst polissamarbete och straffrättsligt samarbete och att det varken harmoniserade frågan om tillgång till uppgifter genom de nationella behöriga myndigheterna eller användning och utbyte av uppgifterna mellan dessa myndigheter. Den drog därför slutsatsen att direktivet i allt väsentligt riktade sig till

---

[10] Artikel 11 i direktiv 2006/24/EG föreskriver följande: I artikel 15 i direktiv 2002/58/EG skall följande punkt införas:”1a. Punkt 1 skall inte tillämpas på uppgifter som specifikt skall lagras enligt Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät för de ändamål som avses i artikel 1.1 i det direktivet.”

[11] Artikel 29-gruppen ifrågasätter om det var meningen att direktiv 2006/24/EG skulle avvika från den allmänna skyldigheten att radera trafikuppgifter efter det att den elektroniska kommunikationen hade avslutats eller ge alla uppgiftslämnare som redan hade behörighet att lagra uppgifter för egna affärsändamål i uppgift att lagra dessa.

operatörernas verksamhet i den relevanta sektorn på den inre marknaden. Domstolen godkände följaktligen den rättsliga grunden[12].

3.3. Bevarande av uppgifter

Lagring av uppgifter skiljer sig från bevarande av uppgifter (eller frysning av kommunikationsuppgifter) enligt vilken operatörer som delgivits ett rättsligt avgörande är skyldiga att lagra uppgifter som avser särskilda individer som misstänks för brottslig verksamhet från och med dagen för beslutet om frysning. Frysning av uppgifter är ett av de undersökningsredskap som planeras och används av de stater som deltar i Europarådets konvention mot cyberbrott[13]. Nästan alla deltagande stater har inrättat en kontaktpunkt, vars roll är att garantera omedelbart ingripande i cyberbrottutredningar eller cyberbrottsförfaranden. Inte alla parter i konventionen förefaller ha garanterat frysning av uppgifter och ingen utvärdering har ännu gjorts av hur effektiv modellen har varit vad gäller att hantera cyberbrott[14]. En ny typ av frysning av uppgifter kallad *quick freeze plus* har nyligen utvecklats. Denna modell går vidare än den tidigare frysningen av uppgifter då också en domare kan bevilja tillgång till uppgifter som operatörerna ännu inte har raderat. Det kommer enligt lagstiftningen också att finnas ett mycket begränsat undantag från skyldigheten att radera vissa kommunikationsuppgifter som vanligtvis inte lagras, under en kort tidsperiod, såsom lokaliseringsuppgifter, uppgifter om internetanslutning och dynamiska IP-adresser för användare som har abonnemang med fast pris och där det inte finns något behov av att lagra uppgifter för faktureringsändamål.

De som rekommenderar frysning av uppgifter menar att denna utgör en lägre grad av intrång i privatlivet än lagringen av uppgifter. De flesta medlemsstater instämmer dock inte i att eventuella variationer i frysningen av uppgifter i tillräcklig grad kan ersätta lagring av uppgifter, genom att hävda att även om lagring av uppgifter leder till att historiska uppgifter finns tillgängliga ger inte frysningen av uppgifter någon garanti för att det kan fastställas bevis innan beslut om frysning har fattats, att en utredning kan inledas i de fall där målet för brottet inte är känt eller att bevis kan samlas in om hur offer eller vittnen till brott[15] förflyttar sig.

4. INFÖRLIVANDE AV DIREKTIV 2006/24/EG

Medlemsstaterna ålades att införliva direktivet innan den 15 september 2007, med valet att till den 15 mars 2009 uppskjuta genomförandet av lagringsskyldigheterna avseende internetåtkomst, internetbaserad e-post och internettelefoni.

Den analys som följer bygger på anmälningar avseende införlivandet som kommissionen har tagit emot från 25 medlemsstater, inbegripet Belgien som bara delvis har införlivat

---

12 EU-domstolen, C-301/6 Irland mot parlamentet och rådet, REG 2009, s. I-00593.

13 Artikel 16 i konventionen om cyberbrott (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

14 Källa: Europarådet.

15 Detta erkändes också i den tyska författningsdomstolens dom i vilken den ogiltigförklarade den tyska lagen om införlivande av direktivet (se avsnitt 4.9) (*Bundesverfassungsgericht, 1 BvR* 256/08 av den 2 mars 2010, punkt 208).

direktivet[16]. I Österrike och Sverige håller utkast till lagstiftning på att diskuteras. I dessa två medlemsstater finns ingen skyldighet att lagra uppgifter men brottsbekämpande myndigheter kan begära och begär att få tillgång till trafikuppgifter från operatörer i den utsträckning dessa uppgifter finns tillgängliga. Efter Tjeckiens, Tysklands och Rumäniens ursprungliga anmälan om införlivande ogiltigförklarade författningsdomstolarna den inhemska lagstiftningen om införlivande av direktivet[17]. Dessa överväger nu hur man igen ska införliva direktivet.

I detta avsnitt analyseras hur medlemsstaterna har införlivat de relevanta bestämmelserna i direktivet. I avsnittet analyseras också om medlemsstaterna har valt att ersätta operatörerna för de kostnader som har uppstått vid lagring och hämtning av uppgifter, för vilka det inte finns några bestämmelser i direktivet, och tar upp direktivets relevans för domarna i Tysklands, Rumäniens och Tjeckiens författningsdomstolar.

4.1. Syftet med lagring av uppgifter (artikel 1)

Genom direktivet åläggs medlemsstaterna att anta åtgärder som säkerställer att uppgifter lagras och finns tillgängliga i syfte att utreda, upptäcka och åtala grova brott, enligt definitionen i var och en av medlemsstaternas nationella lagstiftning. De syften som anges för att lagra och/eller hämta uppgifter fortsätter att variera i EU. Tio medlemsstater (Bulgarien, Estland, Irland, Grekland, Spanien, Litauen, Luxemburg, Ungern, Nederländerna och Finland) har definierat *grova brott* genom att hänvisa till ett minsta fängelsestraff, möjligheten att ett fängelsestraff utdöms eller en förteckning över grova brott som definieras någon annanstans i den nationella lagstiftningen. Åtta medlemsstater (Belgien, Danmark, Frankrike, Italien, Lettland, Polen, Slovakien och Slovenien) kräver att uppgifter inte bara ska lagras för att utreda, upptäcka och åtala grova brott, utan också vid alla straffbara gärningar och för att förhindra brott, eller av mer allmänna skäl som nationell, statlig och/eller allmän säkerhet. Fyra medlemsstaters lagstiftning (Cypern, Malta, Portugal och Förenade kungariket) hänvisar till *grovt brott* eller allvarlig överträdelse utan att definiera dem. Närmare uppgifter finns i tabell 1.

Tabell 1: Ändamålsbegränsning avseende lagring av uppgifter som anges i nationell lagstiftning	
Belgien	För att utreda och åtala straffbara gärningar, åtal av missbruk av nödnummertjänster, utredning av uppsåtligt missbruk av elektroniska kommunikationsnät eller kommunikationstjänster, uppdrag för att samla in underrättelser som görs av underrättelse- och säkerhetstjänster[18].

[16] De 25 medlemsstater som har anmält införlivandet av direktivet till kommissionen är Belgien, Bulgarien, Tjeckien, Danmark, Tyskland, Grekland, Estland, Irland, Spanien, Frankrike, Italien, Cypern, Lettland, Litauen, Luxemburg, Ungern, Malta, Nederländerna, Polen, Portugal, Rumänien, Slovenien, Slovakien, Finland och Förenade kungariket. Belgien underrättade kommissionen att utkast till lagstiftning för att fullborda införlivandet fortfarande ligger kvar hos parlamentet.

[17] Rumänska författningsdomstolens beslut nr 1258 av den 8 oktober 2009, Rumäniens officiella tidning nr 789 av den 23 november 2009. *Bundesverfassungsgerichts* dom 1 BvR 256/08 av den 2 mars 2010, Officiella tidningen av den 1 april 2011. Författningsdomstolens dom av den 22 mars om bestämmelserna i avsnitt 97 punkterna 3 och 4 i lag nr 127/2005 Coll. om elektroniska kommunikationer och om ändring av vissa därtill hörande rättsakter som ändrats, och förordning nr 485/2005 Coll. om lagring av uppgifter och överföring av uppgifter till behöriga myndigheter.

[18] Artikel 126.1 i lagen av den 13 juni 2005 om elektronisk kommunikation.

Tabell 1: Ändamålsbegränsning avseende lagring av uppgifter som anges i nationell lagstiftning	
Bulgarien	För att upptäcka och utreda grova brott och brott som omfattas av artikel 319a–319f i strafflagstiftningen samt för att söka efter personer[19].
Tjeckien	Inte införlivat.
Danmark	För utredning och lagföring av brott och straffbara gärningar[20].
Tyskland	Inte införlivat.
Estland	Får användas om insamlingen av bevismaterial genom annat procedurbeslut förhindras eller är särskilt komplicerad och ändamålet med ett straffrättsligt förfarande är en straffbar gärning [av första graden eller ett uppsåtligt brott av andra graden med fängelsestraff på minst tre år][21].
Irland	För att förhindra grova brott [dvs. brott som leder till fängelsestraff på minst fem år eller ett brott som ingår i tidsplanen för lagen om införlivande], skydd av statens säkerhet, rädda människoliv[22].
Grekland	I syfte att upptäcka särskilt grova brott[23].
Spanien	För utredning, avslöjande och åtal av grova brott som behandlas i strafflagen eller i särskild straffrättslig lagstiftning[24].
Frankrike	För utredning, avslöjande och åtal av grova brott och enbart för att förse rättsliga myndigheter med de uppgifter de behöver och för att förhindra terroristhandlingar och skydd av immaterialrätt[25].
Italien	För att upptäcka och förhindra straffbara gärningar[26].
Cypern	För att utreda grova brott[27].

19 Artikel 250a.2 i lagen om elektroniska kommunikationer (ändrad) 2010.
20 Artikel 1 i *Data Retention Order*.
21 Underavsnitt 110.1 i straffprocesslagen.
22 Artikel 6 i kommunikationslagen (*Retention of Data Act*) 2011.
23 Dessa brott definieras i artikel 4 i lag nr 2225/1994 och artikel 1 i lag nr 3917/2011.
24 Artikel 1.1 i lag nr 25/2007.
25 Följande rättsakter reglerar användningen av lagrade uppgifter för straffbara gärningar, för att förhindra terroristhandlingar och skydd av immaterialrätt: Artikel L.34-1(II), CPCE, lag nr 2006-64 av den 23 januari 2006 och lag nr 2009-669 av den 12 juni 2009.
26 Artikel 132.1 i lagen om dataskydd.
27 Artikel 4.1 i lag nr 183(I)/2007.

Tabell 1: Ändamålsbegränsning avseende lagring av uppgifter som anges i nationell lagstiftning	
Lettland	För skydd av nationell och allmän säkerhet eller för att säkra utredning av grova brott, straffrättsliga förfaranden och straffrättsliga påföljder[28].
Litauen	För att utreda, avslöja och åtala grova och mycket grova brott enligt definitionen i Litauens strafflagstiftning[29].
Luxemburg	För att upptäcka, utreda och avslöja grova brott med ett maxtraff på ett år eller mer[30].
Ungern	För att ge undersökningsorgan, åklagarmyndigheten, domstolarna och nationella säkerhetsorgan möjlighet att utföra sina uppgifter och ge polismyndigheten samt tull- och finansinspektionen möjlighet att undersöka uppsåtliga brott med fängelsestraff på två år eller mer[31].
Malta	För att utreda, avslöja och åtala grova brott[32].
Nederländerna	För utredning och åtal av grova brott där häktning kan ingå[33].
Österrike	Inte införlivat.
Polen	För att förhindra eller upptäcka brott, förhindra eller upptäcka skattebrott, för att användas av åklagarmyndigheter och domstolar om det är av relevans för det domstolsförfarande som väntar, för att den interna säkerhetsbyrån, underrättelsetjänsten, byrån för korruptionsbekämpning, militära kontraspionagetjänster och militära underrättelsetjänster ska kunna utföra sina uppgifter[34].
Portugal	För att utreda, avslöja och åtala grova brott[35].
Rumänien	Inte införlivat.

28 Artikel 71.1 i lagen om elektronisk kommunikation.
29 Artikel 65 i lag X-1835.
30 Artikel 1.1 i lagen av den 24 juli 2010.
31 Lagring av uppgifter för allmänna ändamål: artikel 159/A i lag C/2003, ändrad genom lag CLXXIV/2007. Lagring av uppgifter för polismyndighetens tillgång: artikel 68 i rättsakt XXXIV/1994. Lagring för att ge tull- och finansinspektionen tillgång: artikel 59 i lag CXXII/2010.
32 Artikel 20.1 i det rättsliga meddelandet nr 198/2008.
33 Artikel 126 i straffprocesslagen.
34 Artikel 180a i telekommunikationslagen av den 16 juli 2004, ändrad genom artikel 1 i rättsakten av den 24 april 2009.
35 Artiklarna 1 och 3.1 i lag nr 32/2008.

Tabell 1: Ändamålsbegränsning avseende lagring av uppgifter som anges i nationell lagstiftning	
Slovenien	För att säkerställa nationell säkerhet, grundlagsreglering och säkerhet, statens politiska och ekonomiska intressen samt nationellt försvar[36].
Slovakien	För att förebygga, undersöka, avslöja brott eller åtala brott[37].
Finland	För att utreda, upptäcka och åtala grov brottslighet som anges i kapitel 5a, artikel 3.1 i tvångsmedelslagen[38].
Sverige	Inte införlivat.
Förenade kungariket	För att utreda, avslöja och åtala grova brott[39].

Merparten av de medlemsstater som införlivat direktivet ger, i enlighet med sin lagstiftning, tillgång till och användning av lagrade uppgifter för ändamål som sträcker sig utöver dem som anges i direktivet, inbegripet förebyggande och bekämpning av brott generellt samt risker som är livshotande. Även om detta tillåts enligt direktiv 2002/58/EG är den harmoniseringsnivå som uppnåtts genom EU-lagstiftningen på området fortfarande begränsad. Skillnaderna vad gäller ändamålet med lagringen av uppgifter kommer sannolikt att påverka mängden ansökningar och hur ofta ansökningarna lämnas och i sin tur de kostnader som uppstår för att uppfylla skyldigheterna i direktivet. Denna situation kan visa sig vara otillräcklig för den förutsägbarhet som är ett krav i eventuella lagstiftningsåtgärder som begränsar rätten till integritet[40]. Kommissionen kommer att bedöma behovet av, och alternativen för att uppnå en ökad nivå av harmonisering på området[41].

4.2. Operatörerna åläggs att uppfylla kravet på lagring av uppgifter (artikel 1)

Direktivet är tillämpligt på ”leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät” (artikel 1.1). Två medlemsstater (Finland och Förenade kungariket) kräver inte att små operatörer ska lagra uppgifter, eftersom de anser att kostnaderna för lagringen för både leverantörerna och staten är högre än fördelarna för straffrättssystemen och brottsbekämpningen. Fyra medlemsstater (Lettland,

---

36 Artikel 170.a 1 i lagen om elektronisk kommunikation.

37 Artikel 59a.6 i lagen om elektronisk kommunikation.

38 Artikel 14a.1 i lagen om elektronisk kommunikation.

39 Förordningarna om lagring av uppgifter (EG-direktiv) från 2009 (2009 nr 859).

40 EU-domstolens dom av den 20 maj 2003 i de förenade målen C-465/00, C-138/01 och C-139/01 (Begäran om förhandsavgörande framställd av *Verfassungsgerichtshof* och *Oberster Gerichtshof*): Rechnungshof (C-465/00) mot Österreichischer Rundfunk m.fl. och mellan Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) och Österreichischer Rundfunk (Skydd för enskilda personer med avseende på behandling av personuppgifter — Direktiv 95/46/EG — Skydd av privatlivet — Utlämnande av uppgifter om vilka inkomster som anställda vid organ som står under tillsyn av Rechnungshof har).

41 När direktivet antogs utfärdade kommissionen en förklaring där den föreslog att förteckningen över brott i Europeiska arresteringsordern borde övervägas. (Rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna.)

Luxemburg, Nederländerna och Polen) rapporterar att de har infört alternativa administrativa arrangemang. Medan stora operatörer som är närvarande i flertalet medlemsstater gynnas av stordriftsfördelar när det gäller kostnaderna har mindre operatörer i vissa medlemsstater haft en tendens att bilda gemensamma företag eller lägga ut verksamheten på entreprenad till företag som specialiserat sig på lagrings- och hämtningsfunktioner för att minska sina kostnader. Att på detta sätt lägga ut tekniska funktioner på entreprenad påverkar inte leverantörernas skyldighet att på lämpligt sätt övervaka bearbetningen och säkerställa att de krävda säkerhetsåtgärderna finns på plats, vilket kan bli särskilt problematiskt för mindre operatörer. Kommissionen kommer att undersöka frågorna om uppgifternas säkerhet, och deras inverkan på små och medelstora företag, i förhållande till alternativen för att ändra ramverket om lagring av uppgifter.

4.3. Åtkomst till uppgifter: myndigheter, förfaranden och villkor (artikel 4)

Medlemsstaterna uppmanas att säkerställa att [lagrade uppgifter] bara levereras till behöriga nationella myndigheter i specifika ärenden och i enlighet med nationell lagstiftning. Varje enskild medlemsstat ska i den nationella lagstiftningen fastställa de förfaranden som ska följas och de villkor som ska uppfyllas för att erhålla tillgång till lagrade uppgifter i enlighet med nödvändighets- och proportionalitetskraven, och följa tillämpliga bestämmelser i EU-lagstiftningen och folkrätten, särskilt Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, i enlighet med den tolkning som görs av Europeiska domstolen för mänskliga rättigheter.

I alla medlemsstater kan de nationella polisstyrkorna och, utom i rättssystem som är baserade på sedvanerätt (Irland och Förenade kungariket), åklagarmyndigheter, få åtkomst till lagrade uppgifter. Fjorton medlemsstater förtecknar säkerhets- eller underrättelsetjänster eller militärsektorn bland de behöriga myndigheterna. Sex medlemsstater förtecknar skatte- och/eller tullmyndigheter och tre medlemsstater förtecknar gränsbevakande myndigheter. En medlemsstat tillåter andra offentliga myndigheter få tillgång till uppgifterna om de enligt sekundärlagstiftningen ges tillåtelse för särskilda ändamål. Elva medlemsstater kräver rättsligt bemyndigande för varje ansökan om tillgång till lagrade uppgifter. I tre medlemsstater krävs rättsligt bemyndigande i de flesta fall. Fyra andra medlemsstater kräver bemyndigande från en högre överordnad, men inte en domare. I två medlemsstater förefaller det enda villkoret vara att ansökan lämnas i skriftlig form.

Tabell 2: Tillgång till lagrade telekommunikationsuppgifter		
	Behöriga nationella myndigheter	*Förfaranden och villkor*
Belgien	Enhet för rättslig samordning, rannsakningsdomare, åklagarmyndighet och kriminalpolis.	Tillgång måste bemyndigas av en domare eller åklagare. På begäran ska operatörerna lämna abonnent-, trafik- och lokaliseringsuppgifter i realtid för samtal som har gjorts under den senaste månaden. Uppgifter för äldre samtal ska lämnas så

Tabell 2: Tillgång till lagrade telekommunikationsuppgifter		
	Behöriga nationella myndigheter	*Förfaranden och villkor*
		snart som möjligt.
Bulgarien[42]	Särskilda direktorat och avdelningar i det statliga organet för nationell säkerhet, inrikesministeriet, den militära underrättelsetjänsten, militärpolistjänsten, försvarsministeriet och det nationella undersökningsorganet, domstol och förundersökningsmyndigheter.	Tillgång bara möjlig efter bemyndigande av ordföranden i en distriktsdomstol.
Tjeckien	Inte införlivat.	
Danmark[43]	Polismyndighet.	Tillgång kräver rättsligt bemyndigande. Domstolsbeslut beviljas om ansökan uppfyller strikta kriterier om misstankar, behov och proportionalitet.
Tyskland	Inte införlivat.	
Estland[44]	Polismyndighet och gränsbevakningsmyndigheten, säkerhetspolisen samt skatte- och tullmyndigheten när det gäller föremål och elektronisk kommunikation.	Tillgång kräver tillåtelse av en preliminär undersökningsdomare. Operatörerna måste lämna [lagrade uppgifter] inom tio timmar och i andra fall inom tio arbetsdagar [efter mottagandet av ansökan].
Irland[45]	Medlemmar i Garda Síochána (polisen) på kommissarienivå eller högre. Officerare i permanenta försvarsstyrkor på överstenivå eller högre. Tjänstemän på skattemyndigheten på förste handläggarnivå eller högre.	Ansökningar ska lämnas i skriftlig form.
Grekland[46]	Offentliga rättsliga, militära eller polisiära myndigheter.	Tillgång kräver rättsligt avgörande som förklarar att det är omöjligt eller ytterst svårt att göra undersökningar på annat sätt.
Spanien[47]	Polisstyrkor med ansvar för att upptäcka, utreda och åtala grova brott, den nationella underrättelsetjänsten och tullmyndigheter.	De behöriga nationella myndigheternas tillgång till dessa uppgifter kräver förhandsgodkännande av domstol.
Frankrike[48]	Åklagarmyndighet, utsedda polisofficerare och gendarmer.	Polisen måste motivera varje ansökan om tillgång till lagrade uppgifter och söka tillstånd från en person i inrikesministeriet som utsetts av *Commission nationale de contrôle des interceptions de sécurité*. Ansökningar om tillgång handläggs av en tjänsteman som är anställd av operatören.
Italien[49]	Åklagarmyndighet, polismyndighet, försvarare för endera svaranden eller den person som berörs av utredningen.	Tillgång kräver ett motiverat beslut som utfärdas av åklagarmyndigheten.
Cypern[50]	Domstol, åklagarmyndighet och polis.	Tillgången måste godkännas av en åklagare om denne anser att åtgärden kan

42 Artikel 250b.1 i lagen om elektroniska kommunikationer (ändrad) 2010 (myndigheter). Artikel 250b.1 och 250c.1 i lagen om elektroniska kommunikationer (ändrad) 2010 (tillgång).

43 Artikel 71 i rättsakt om domstolssystemet.

44 Underavsnitt 112.2 och 112.3 i straffprocesslagen (om myndigheter och förfaranden). Underavsnitt 111.9 (villkor) i lagen om elektronisk kommunikation.

45 Artikel 6 i kommunikationslagen 2009.

46 Artiklarna 3 och 4 i lag nr 2225/94.

47 Artiklarna 6–7 i lag nr 25/2007.

48 Artiklarna 60.1 och 60.2 i straffprocesslagen (myndigheter), artikel L.31-1-1 (villkor).

49 Artikel 132.3 i lagen om dataskydd

Tabell 2: Tillgång till lagrade telekommunikationsuppgifter		
	Behöriga nationella myndigheter	*Förfaranden och villkor*
		ge bevisning för att ett grovt brott har begåtts. En domare kan utfärda ett sådant bemyndigande om det finns en rimlig misstanke om att ett grovt brott har begåtts och om uppgifterna sannolikt kan kopplas till det.
Lettland[51]	Behöriga tjänstemän i institutioner som bedriver förundersökningar. Personer som bedriver undersökningsarbete. Behöriga tjänstemän i institutioner för statens säkerhet, åklagarmyndighet och domstol.	Behöriga tjänstemän, åklagarmyndigheten och domstol ska bedöma ansökningarnas korrekthet och relevans, registrera ansökan och garantera uppgifternas säkerhet. Behöriga organ kan underteckna ett avtal med en operatör för t.ex. kryptering av uppgifter.
Litauen[52]	Organ som bedriver förundersökningar, åklagaren, domstol (domare) och underrättelsetjänstemän.	Behöriga offentliga myndigheter måste skriftligen begära lagrade uppgifter. För tillgång till förundersökningar krävs en domstolsorder.
Luxemburg[53]	Rättsliga myndigheter (undersökningsdomare, åklagare), myndigheter ansvariga för nationell säkerhet, försvar, allmän säkerhet och förhindrande, undersökning, upptäckt och åtal av brottsliga gärningar.	Tillgång kräver rättsligt bemyndigande.
Ungern[54]	Polismyndighet, nationella skatte- och tullmyndigheter, nationella säkerhetsorgan, åklagarmyndighet och domstol.	Polis och nationella skatte- och tullmyndigheter kräver åklagares bemyndigande. Åklagaren och de nationella säkerhetsorganen kan få tillgång till dessa uppgifter utan domstolsbeslut.
Malta[55]	Maltas poliskår och säkerhetstjänst.	Ansökningar ska lämnas i skriftlig form.
Nederländerna[56]	Undersökande polistjänsteman.	Tillgång ges genom beslut från åklagare eller en undersökningsdomare.
Österrike	Inte införlivat.	
Polen[57]	Polismyndighet, gränsbevakande myndigheter, skatteinspektörer, internt säkerhetsorgan, underrättelsetjänsten, byrån för korruptionsbekämpning, militära kontraspionagetjänster, militär underrättelsetjänst, domstol och åklagarmyndigheten.	Ansökningarna ska lämnas skriftligen och, när det gäller polismyndigheter, gränsbevakande myndigheter och skatteinspektörer, bemyndigas av en högre tjänsteman i organisationen.

50 Artiklarna 4.2 och 4.4 i lag nr 183(I)/2007.

51 Artikel 71.1 i lagen om elektronisk kommunikation (myndigheter). Kansliförordning nr 820 (förfaranden).

52 Artiklarna 77.1 och 77.2 i lag nr X-1835, muntlig rapport till kommissionen.

53 Artiklarna 5-2.1 och 9.2 i lagen av den 24 juli 2010 (myndigheter), artikel 67.1 i straffprocesslagen (villkor).

54 Artiklarna 68.1 och 69.1 c och d i rättsakt XXXIV 1994, artiklarna 9/A.1 i rättsakt V 1972, artiklarna 71.1, 71.3, 71.4, 178/A.4, 200, 201, 268.2 i rättsakt XIX 1998, artiklarna 40.1, 40.2, 53.1, 54.1 j i rättsakt CXXV 1995.

55 Artiklarna 20.1 och 20.3 i det rättsliga meddelandet nr 198/2008.

56 Artikel 126ni i straffprocesslagen.

57 Artikel 179.3 i telekommunikationslagen av den 16 juli 2004, ändrad genom artikel 1 i rättsakten av den 24 april 2009.

Tabell 2: Tillgång till lagrade telekommunikationsuppgifter		
	Behöriga nationella myndigheter	*Förfaranden och villkor*
Portugal[58]	Kriminalpolis, republikanska nationalgardet, allmänt säkerhetskontor, militär rättspolis, avdelning för utlännings- och gränsbevakning, sjöpolis.	Överföring av uppgifter kräver rättsligt bemyndigande med motiveringen att det är väsentligt och uppfyller villkoren om behov och proportionalitet. Det rättsliga bemyndigandet ska omfattas av kravet på nödvändighet och proportionalitet.
Rumänien	Inte införlivat.	
Slovenien[59]	Polismyndighet, underrättelse- och säkerhetsorgan, försvarsorgan med ansvar för underrättelse- och kontraspionagetjänster och säkerhetsuppdrag.	Tillgång kräver rättsligt bemyndigande.
Slovakien[60]	Myndigheter med ansvar för brottsbekämpning och domstolar.	Ansökningar ska lämnas i skriftlig form.
Finland[61]	Polismyndighet, gränsbevakning, tullmyndigheter (för lagrade abonnent-, trafik- och lokaliseringsuppgifter). Centrum för krisberedskap, sjöräddningsverksamhet, underavdelning i sjöräddningen (för identifiering och lokalisering av uppgifter i krissituationer).	Abonnentuppgifter kan fås av alla behöriga myndigheter utan rättsligt bemyndigande. Andra uppgifter kräver domstolsbeslut.
Sverige	Inte införlivat.	
Förenade kungariket[62]	Polismyndighet, underrättelsetjänst, skatte- och finansmyndigheter, andra offentliga myndigheter som utsetts genom sekundärlagstiftningen.	Tillgång tillåten, efter tillstånd från en utnämnd person, och behovs- och proportionalitetstest, i särskilda fall och omständigheter där avslöjande av uppgifter tillåts eller krävs enligt lag. Man har kommit överens om särskilda förfaranden med operatörerna.

Kommissionen kommer att bedöma behovet av och alternativen för att uppnå en ökad harmoniseringsgrad med hänsyn till vilka myndigheter som ska få tillgång, och vilka förfaranden som ska gälla för att få tillgång till lagrade uppgifter. Detta kan komma att inbegripa mer klart definierade förteckningar över behöriga myndigheter, oberoende och/eller rättslig tillsyn av ansökningar om uppgifter och minimikrav vad gäller operatörernas förfaranden för att bevilja behöriga myndigheter tillgång.

4.4. Tillämpningsområdet för lagring av uppgifter och de kategorier av uppgifter som omfattas (artiklarna 1.2, 3.2 och 5)

Direktivet tillämpas på områdena fast telefoni, mobil telefoni, internetåtkomst, internetbaserad e-post och internettelefoni. Det anger (i artikel 5) de kategorier av uppgifter som ska lagras, nämligen uppgifter som behövs för att identifiera:

---

58 Artiklarna 2.1, 3.2 och 9 i lag nr 32/2008.

59 Artikel 107c i lagen om elektronisk kommunikation, artikel 149b i straffprocesslagen, artikel 24.b i *Intel and Security Agency Act*, artikel 32 i försvarsakten.

60 Artikel 59a.8 i lagen om elektronisk kommunikation.

61 Artiklarna 35.1 och 36 i lagen om elektronisk kommunikation, artikel 31–33 i polislagen, artikel 41 i gränsbevakningslagen.

62 Artikel 25, *Schedule 1, Regulation of Investigatory Powers Act* 2000, artikel 7 i *Data Retention Regulation*, artikel 22.2 i lagen om införlivande (*RIPA)* anger de ändamål för vilka myndigheterna kan få tillgång till uppgifter.

1.1. Kommunikationskälla.

1.2. Kommunikationens destination.

1.3. Datum, tidpunkt och varaktighet för en kommunikation.

1.4. Typ av kommunikation.

1.5. Användarnas kommunikationsutrustning eller den utrustning som tros ha använts.

1.6. Lokaliseringen av mobil kommunikationsutrustning.

Det omfattar också misslyckade uppringningsförsök (artikel 3.2), dvs. en kommunikation där ett telefonsamtal har kopplats men inte besvarats eller där nätadministrationen har ingripit och där uppgifter om dessa försök genererats, behandlats, lagrats eller loggats av operatörer. Inga uppgifter som avslöjar kommunikationens innehåll får lagras i enlighet med detta direktiv. Det har också klargjorts att sökningar, dvs. serverloggar som genereras genom en sökmotortjänst, också ligger utanför direktivets tillämpningsområde, eftersom de snarare anses utgöra innehåll än trafikuppgifter[63].

21 medlemsstater föreskriver lagring av var och en av dessa kategorier av uppgifter i sina lagar om införlivande. Belgien har inte föreskrivit lagring av telefoniuppgifter, inte heller vad gäller internetrelaterade uppgifter. De som svarade på kommissionens frågeformulär ansåg det inte vara nödvändigt att ändra de kategorier av uppgifter som ska lagras, även om Europaparlamentet har utfärdat en skriftlig förklaring där den uppmanar kommissionen att utvidga direktivet till att omfatta sökmotorer för att snabbt kunna hantera barnpornografi online och sexuella övergrepp[64]. I sin rapport om den andra brottsbekämpningsåtgärden gjorde artikel 29-gruppen gällande att de kategorier som anges i direktivet bör anses vara uttömmande, utan att operatörerna åläggs några ytterligare skyldigheter om lagring av uppgifter. Kommissionen kommer att bedöma om alla dessa kategorier av uppgifter är nödvändiga.

4.5. Lagringsperioder (artikel 6 och artikel 12)

Medlemsstaterna ska säkerställa att de kategorier av uppgifter som anges i artikel 5 lagras under en period av minst 6 och högst 24 månader. Den högsta tillåtna lagringsperioden kan förlängas av en medlemsstat som står inför särskilda omständigheter som föranleder en tidsbegränsad förlängning. En sådan förlängning ska anmälas till kommissionen som inom sex månader efter mottagandet av anmälan ska fatta beslut om förlängningen ska godkännas eller avslås. Även om den högsta tillåtna lagringsperioden kan förlängas finns det inga bestämmelser för att förkorta lagringen till mindre än sex månader. Alla medlemsstater som har införlivat direktivet, utom en, tillämpar en lagringspriod eller lagringsperioder inom dessa gränser och kommissionen har inte tagit emot några anmälningar om förlängning. Det finns dock ingen metod som konsekvent används i EU.

---

63 Artikel 29-gruppens yttrande om uppgiftsskyddsfrågor relaterade till sökmotorer av den 4 april 2008.

64 Skriftlig förklaring i enlighet med artikel 123 i arbetsordningen om inrättandet av ett europeiskt system för tidig varning för pedofiler och sexualbrottslingar, 19.4.2010, 0029/2010.

Femton medlemsstater anger en enda period för alla kategorier av uppgifter: en medlemsstat (Polen) anger en lagringsperiod på 24 månader, en anger 18 månader (Lettland), tio anger 12 månader (Bulgarien, Danmark, Estland, Grekland, Spanien, Frankrike, Nederländerna, Portugal, Finland och Förenade kungariket) och tre anger 6 månader (Cypern, Luxemburg och Litauen). Fem medlemsstater har fastställt olika lagringsperioder för olika kategorier av uppgifter: två medlemsstater (Irland och Italien) anger 24 månader för uppgifter om fast och mobil telefoni och 12 månader för internetåtkomst, internetbaserad e-post och internettelefoni. En medlemsstat (Slovenien) anger 14 månader för telefoniuppgifter och åtta månader för internetrelaterade uppgifter. En medlemsstat (Slovakien) anger 12 månader för fast och mobil telefoni och 6 månader för internetrelaterade uppgifter. En medlemsstat (Malta) anger 12 månader för uppgifter om fast telefoni, mobil telefoni och internettelefoni och 6 månader för internetåtkomst och internetbaserad e-post. En medlemsstat (Ungern) lagrar alla uppgifter i 12 månader, utom uppgifter om misslyckade uppringningsförsök som bara lagras under 6 månader. En medlemsstat (Belgien) har inte specificerat någon lagringsperiod för de kategorier av uppgifter som anges i direktivet. Närmare uppgifter finns i tabell 3.

Tabell 3: Lagringsperioder som anges i nationell lagstiftning	
Belgien[65]	Mellan 12 och 36 månader för allmänt tillgängliga telefonitjänster. Ingen bestämmelse för internetrelaterade uppgifter.
Bulgarien	12 månader. Uuppgifter som man fått tillgång till får på begäran lagras under ytterligare 6 månader.
Tjeckien	Inte införlivat.
Danmark	12 månader.
Tyskland	Inte införlivat.
Estland	12 månader.
Irland	24 månader för uppgifter för telefoni i fasta nät och mobil telefoni och 12 månader för internetåtkomst, internetbaserad e-post och internettelefoni.
Grekland	12 månader.
Spanien	12 månader.
Frankrike	12 månader.
Italien	24 månader för uppgifter för telefoni i fasta nät och mobil telefoni och 12 månader för internetåtkomst, internetbaserad e-post och internettelefoni.
Cypern	6 månader.
Lettland	18 månader.
Litauen	6 månader.
Luxemburg	6 månader.
Ungern	6 månader för misslyckade uppringningsförsök och 12 månader för alla andra uppgifter.
Malta	12 månader för uppgifter i fasta telefonnät, mobil telefoni och internettelefoni och 6 månader för internetåtkomst och internetbaserad e-post.
Nederländerna	12 månader.
Österrike	Inte införlivat.
Polen	24 månader.
Portugal	12 månader.
Rumänien	Inte införlivat (6 månader enligt den tidigare upphävda lagen om införlivande).
Slovenien	14 månader för telefoniuppgifter och 8 månader för internetrelaterade uppgifter.

[65] Artikel 126.2 i lagen av den 13 juni 2005 om elektronisk kommunikation.

Tabell 3: Lagringsperioder som anges i nationell lagstiftning	
Slovakien	12 månader för uppgifter för telefoni i fasta nät och mobil telefoni, 6 månader för internetåtkomst, internetbaserad e-post och internettelefoni.
Finland	12 månader.
Sverige	Inte införlivat.
Förenade kungariket	12 månader.

Även om denna mångfald av tillvägagångssätt tillåts i direktivet ges i direktivet bara begränsad rättssäkerhet och förutsägbarhet för operatörer i EU som bedriver verksamhet i mer än en medlemsstat och för medborgare vars kommunikationsuppgifter kan lagras i olika medlemsstater. Mot bakgrund av den växande internationaliseringen vad gäller bearbetning av uppgifter och outsourcing av lagring av uppgifter, bör man överväga alternativ för att harmonisera lagringsperioderna i EU. För att uppfylla proportionalitetsprincipen och för att belysa utvecklingen inom kommunikation och teknik samt brott och terrorism kommer kommissionen att överväga att tillämpa olika perioder för olika kategorier av uppgifter, för olika kategorier av grova brott eller en kombination av de två[66]. Den kvantitativa bevisning som medlemsstaterna hittills har lämnat när det gäller åldern på lagrade uppgifter visar att cirka 90 % av uppgifterna är sex månader gamla eller mindre och cirka 70 % är tre månader gamla eller mindre när de brottsbekämpande myndigheterna lämnar (den ursprungliga) begäran om tillgång (se avsnitt 5.2).

4.6. Uppgiftsskydd, datasäkerhet och tillsynsmyndigheter (artiklarna 7 och 9)

I direktivet åläggs medlemsstaterna att säkerställa att operatörerna minst respekterar fyra principer för datasäkerhet, nämligen att de lagrade uppgifterna ska

1.7. vara av samma kvalitet och omfattas av samma säkerhet och skydd som de uppgifter som finns på nätet [det allmänna kommunikationsnätet],

1.8. omfattas av lämpliga tekniska och organisatoriska åtgärder för att skydda uppgifterna mot oavsiktlig eller olaglig förstörelse, oavsiktlig förlust eller oavsiktlig ändring, eller otillåten eller olaglig lagring, bearbetning, tillgång eller avslöjande,

1.9. omfattas av lämpliga tekniska och organisatoriska åtgärder för att säkerställa att endast särskilt bemyndigad personal ges tillgång till dem, och att de

1.10. ska förstöras vid slutet av lagringstiden, utom de uppgifter där tillgång har medgivits och som har bevarats [för det ändamål som anges i direktivet].

I enlighet med direktiv 95/46/EG och direktiv 2002/58/EG förbjuds operatörerna att bearbeta lagrade uppgifter som omfattas av direktivet för andra ändamål, under förutsättning att uppgifterna i annat fall inte skulle ha lagrats[67]. Medlemsstaterna ska utse en offentlig myndighet som är helt oberoende och ansvarig för övervakningen och tillämpningen av dessa principer. Dessa myndigheter kan vara desamma som de som anges i direktiv 95/46/EG[68].

---

66 I kommissionens förslag till direktiv om lagring av uppgifter 2005 anges en lagringsperiod på 12 månader för telefoniuppgifter och 6 månader för internetuppgifter.

67 Artikel 13.1 i direktiv 95/46/EG.

68 Artikel 28 i direktiv 95/46/EG.

15 medlemsstater har införlivat alla dessa principer i den relevanta lagstiftningen. Fyra medlemsstater (Belgien, Estland, Spanien och Lettland) har införlivat två eller tre av dessa principer men anger inte uttryckligen att uppgifterna ska förstöras i slutet av lagringsperioden. Två medlemsstater (Italien och Finland) föreskriver att uppgifterna ska förstöras. Det är inte klart vilka särskilda tekniska och organisatoriska säkerhetsåtgärder, som stark autentisering och detaljerad loggåtkomstadministration[69] (*access log management*) som har tillämpats. 22 medlemsstater har en tillsynsmyndighet som är ansvarig för att övervaka tillämpningen av principerna. I de flesta fall är detta datatillsynsmyndigheterna. Närmare uppgifter finns i tabell 4.

Tabell 4: Uppgiftsskydd, datasäkerhet och tillsynsmyndigheter

Medlemsstat	*Uppgiftsskydds- och datasäkerhetsbestämmelser i nationell lagstiftning*	*Tillsynsmyndighet*
Belgien	Operatörerna ska garantera att överföringen av uppgifter inte kan uppfångas av en tredje part och att den uppfyller standarderna i Europeiska institutet för telekommunikationsstandarder vad gäller telekommunikationssäkerhet och lagligt uppfångande[70]. Principen om obligatorisk förstörelse av uppgifter i slutet av lagringsperioden verkar inte ha tagits upp.	Institutet för post- och telekommunikationstjänster.
Bulgarien	I lagen om införlivande inbegrips kravet på att genomföra de fyra principerna[71].	Kommissionen för skydd av personuppgifter övervakar bearbetningen och lagringen av uppgifter för att säkerställa att skyldigheterna uppfylls. Parlamentsutskott i nationalförsamlingen – övervakar förfarandena för beviljande och tillgång till uppgifterna.
Tjeckien[72]	Inte införlivat.	
Danmark	Fyra principer föreskrivs [73].	Den nationella IT- och telekomstyrelsen övervakar leverantörer av elektroniska kommunikationsnäts och kommunikationstjänsters skyldighet att garantera att teknisk utrustning och system gör det möjligt för polismyndigheten att få tillgång till uppgifter om telekomtrafiken.
Tyskland	Inte införlivat.	

69 Stark autentisering inbegriper dubbla autentiseringsmekanismer som lösenord plus biometri eller lösenord plus tecken för att garantera fysisk närvaro av den person som är ansvarig för att bearbeta trafikuppgifter. Detaljerad loggåtkomstadministration inbegriper detaljerad spårning av åtkomst och bearbetning genom lagring av loggar som registrerar användaridentitet, åtkomsttid och handlingar som man fått tillgång till.

70 Artikel 6 i den kungliga förordningen av den 9 januari 2003.

71 Artikel 4.1 i lagen om elektroniska kommunikationer (ändrad) 2010.

72 Avsnitt 87.3 och 88 i lag nr 127/2005, ändrad genom lag nr 247/2008, avsnitt 2 i lag nr 336/2005, Avsnitt 3.4 i lag nr 485/2005, avsnitt 28.1 i lag nr 101/2000.

73 Lagen om bearbetning av personuppgifter, dekret nr 714 av den 26 juni 2008 om leverans av elektroniska kommunikationsnät och kommunikationstjänster.

Tabell 4: Uppgiftsskydd, datasäkerhet och tillsynsmyndigheter		
Medlemsstat	*Uppgiftsskydds- och datasäkerhetsbestämmelser i nationell lagstiftning*	*Tillsynsmyndighet*
Estland	I genomförandelagen anges tre av de fyra principerna. Ingen uttrycklig bestämmelse finns vad gäller den fjärde principen, även om varje person vars uppgifter har missbrukats genom övervakningsrelaterad verksamhet kan begära att uppgifterna förstörs genom domstolsbeslut[74].	Ansvarig myndighet är den tekniska övervakningsmyndigheten.
Irland[75]	I lagen om införlivande ingår skyldigheten att genomföra de fyra principerna.	Den domare som utsetts har befogenhet att undersöka och rapportera om hur de behöriga nationella myndigheterna uppfyller bestämmelserna i lagen om införlivande.
Grekland[76]	Lagen om införlivande inbegriper skyldighet att genomföra de fyra principerna, med ytterligare skyldighet för operatörerna att utarbeta och tillämpa en plan för att säkerställa förenlighet genom att utse en chef för datasäkerhet.	Myndigheten för skydd av personuppgifter och personlig integritet i samband med kommunikationstjänster.
Spanien[77]	Datasäkerhetsbestämmelserna omfattar tre av de fyra principerna (de lagrade uppgifternas kvalitet och säkerhet, åtkomst för bemyndigade personer och skydd mot otillåten bearbetning).	Ansvarig myndighet är datasäkerhetsmyndigheten.
Frankrike[78]	I lagen om införlivande ingår skyldigheten att genomföra de fyra principerna.	Den nationella kommissionen för informationsteknologi och medborgerliga friheter (*Commission nationale de l'informatique et des libertés*) övervakar att skyldigheterna uppfylls.
Italien	Inga uttryckliga bestämmelser om säkerhet vad gäller lagrade uppgifter, även om det finns en allmän skyldighet att förstöra eller avidentifiera trafikuppgifter och reglerande bearbetning av lokaliseringsuppgifter[79].	Datasäkerhetsmyndigheten kontrollerar operatörernas efterlevnad av direktivet.
Cypern[80]	Lagen om införlivande omfattar var och en av de fyra principerna.	Kommissionären för skydd av personuppgifter övervakar tillämpningen av lagen om införlivande.
Lettland[81]	Lagen om införlivande omfattar två av principerna: konfidentialitet av och tillåten åtkomst till lagrade uppgifter och förstörelse av uppgifter när lagringsperioden är slut.	Det statliga uppgiftsskyddsinspektoratet övervakar skyddet av personuppgifter i den elektroniska kommunikationssektorn, men inte åtkomst till och bearbetning av lagrade uppgifter.

74 Underavsnitt 111.9 i lagen om elektroniska kommunikationer, underavsnitt 122.2 i straffprocesslagen.

75 Avsnitt 4, 11 och 12 i kommunikationslagen (*Retention of Data Act*) från 2009.

76 Artikel 6 i lag nr 3917/2011.

77 Artikel 8 i lag nr 25/2007, artikel 38.3 i lagen om allmänna telekommunikationer. Lagen (artikel 9) hänvisar till undantag om tillgång till och inställande som anges i grundlag nr 15/1999 om skydd av personuppgifter (artikel 22 och 23).

78 Artikel D.98-5, CPCE, Artikel L-34-1(V), CPCE, artikel 34 i lag nr 78-17, artikel D.9834, CPCE, artikel 11 i lag nr 78–17 av den 6 januari 1978.

79 Artiklarna 123 och 126 i lagen om dataskydd.

80 Artiklarna 14 och 15 i lag nr 183(I)/2007.

81 Artiklarna 4.4 och 71(6–8) i lagen om elektroniska kommunikationer.

Tabell 4: Uppgiftsskydd, datasäkerhet och tillsynsmyndigheter		
Medlemsstat	*Uppgiftsskydds- och datasäkerhetsbestämmelser i nationell lagstiftning*	*Tillsynsmyndighet*
Litauen[82]	I lagen om införlivande anges de fyra principerna.	Det statliga uppgiftsskyddsinspektoratet övervakar genomförandet av lagen om införlivande och är ansvarigt för att förse Europeiska kommissionen med statistik.
Luxemburg[83]	I lagen om införlivande anges de fyra principerna.	Dataskyddsmyndighet.
Ungern[84]	I lagen om införlivande anges de fyra principerna.	Ombudsmannen för uppgiftskydd och informationsfrihet.
Malta[85]	I lagen om införlivande anges de fyra principerna.	Uppgiftsskyddsombud.
Nederländerna[86]	I lagen om införlivande anges de fyra principerna.	Radiokommunikationsorganet övervakar skyldigheter vad gäller internetåtkomst och tillhandahållandet av telekomtjänster. Uppgiftsskyddsmyndigheten övervakar den allmänna bearbetningen av personuppgifter. Detaljerna vad gäller samarbetet mellan de två myndigheterna anges i ett protokoll.
Österrike	Inte införlivat.	
Polen	I lagen om införlivande anges de fyra principerna[87].	Dataskyddsmyndighet.
Portugal	I lagen om införlivande anges de fyra principerna[88].	Portugals dataskyddsmyndighet.
Rumänien	Inte införlivat.	
Slovenien[89]	I lagen om införlivande anges de fyra principerna.	Informationsombudet.
Slovakien[90]	I lagen om införlivande anges de fyra principerna.	Den nationella tillsyns- och prissättande myndigheten på området telekommunikationer övervakar skyddet av personuppgifter.
Finland	I lagen om införlivande anges uttryckligen bara kravet att förstöra uppgifter när lagringsperioden är slut[91].	Den finska regleringsmyndigheten för telekommunikationer övervakar operatörernas efterlevnad av bestämmelserna om lagring. Dataskyddsombudsmannen övervakar den allmänna lagligheten i bearbetningen av personuppgifter.
Sverige	Inte införlivat.	

82 Artiklarna 12.5, 66.8 och 66.9 i lagen om elektroniska kommunikationer, ändrad den 14 november 2009.

83 Artikel 1.5 i lagen av den 24 juli 2010.

84 Artikel 157 i lag nr C/2003, ändrad genom lag nr CLXXIV/2007, artikel 2 i dekret nr 226/2003 och lag nr LXIII/1992 om uppgiftsskydd.

85 Artikel 24 i den rättsliga noten nr 198/2008, artikel 40b i lagen om dataskydd (kap. 440).

86 Artikel 13.5 i lagen om telekommunikationer. Den långa rubriken på samarbetsprotokollet är *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens.*

87 Artiklarna 180a och 180e i lagen om telekommunikationer.

88 Artiklarna 7.1, 5 och 11 i lag nr 32/2008, artiklarna 53 och 54 i lagen om skydd av personuppgifter.

89 Artiklarna 107a.6 och 107c i lagen om elektronisk kommunikation.

90 Artikel 59a i lagen om elektronisk kommunikation, artikel S33 i lag nr 428/2002 om skydd av personuppgifter.

91 Artikel 16.3 i lagen om elektronisk kommunikation.

Tabell 4: Uppgiftsskydd, datasäkerhet och tillsynsmyndigheter		
Medlemsstat	*Uppgiftsskydds- och datasäkerhetsbestämmelser i nationell lagstiftning*	*Tillsynsmyndighet*
Förenade kungariket	I lagen om införlivande anges de fyra principerna[92].	Dataskyddsombudet övervakar lagring och/eller bearbetning av kommunikationsuppgifter (och eventuella andra personuppgifter) och lämpliga kontroller vad gäller uppgiftsskydd. Den ansvarige för olovlig avlyssning (en aktiv eller pensionerad högre domare) övervakar förvärvet av kommunikationsuppgifter enligt lagen om införlivande (RIPA) genom de offentliga myndigheterna. Domstolen med utredningsbefogenheter utreder klagomål avseende missbruk av uppgifter om dessa förvärvats under införlivandet av lagstiftningen (RIPA).

Införlivandet av artikel 7 är inkonsekvent. Lagrade uppgifter är potentiellt av mycket personlig och känslig art och höga standarder vad gäller uppgiftsskydd och datasäkerhet måste tillämpas under bearbetning, lagring, hämtning och användning. Dessa ska vara konsekventa och synliga för att minimera riskerna för integritetsintrång och bevara medborgarnas förtroende. Kommissionen kommer att överväga alternativ för att stärka standarderna vad gäller datasäkerhet och uppgiftsskydd, också genom att införa inbyggda skyddsmekanismer för att säkra att dessa standarder uppfylls både när det gäller lagring och överföring. Den kommer också att ta hänsyn till de rekommendationer om minimiskydd och tekniska och organisationsmässiga säkerhetsåtgärder som artikel 29-gruppen lämnade i sin rapport om den andra brottsbekämpningsåtgärden[93].

4.7. Statistik (artikel 10*)*

Medlemsstaterna uppmanas att förse kommissionen med årlig statistik om lagring av uppgifter, som ska inbegripa följande:

– De fall där information skickats till behöriga myndigheter i enlighet med gällande nationell lagstiftning.

– Den tid som förflutit från det datum då uppgifterna lagrades och det datum då den behöriga myndigheten begärde överföring av uppgifterna (dvs. uppgifternas ålder).

– De fall där en begäran om uppgifter inte kunde tillgodoses.

När kommissionen begärde statistik i enlighet med denna bestämmelse uppmanade den medlemsstaten att lämna uppgifter om fall där individuella ansökningar om uppgifter lämnats. Den statistik som lämnades skiljde sig åt vad gäller tillämpningsområde och detaljnivå: vissa medlemsstater gjorde åtskillnad mellan olika typer av kommunikation i sina svar, vissa angav uppgifternas ålder vid tidpunkten för begäran, medan andra bara lämnade årlig statistik utan några detaljer. 19 medlemsstater[94] lämnade statistik om antalet ansökningar om uppgifter under 2009 och/eller 2008. Detta inbegrep Irland, Grekland och Österrike, där uppgifter

---

92 Artikel 6 i *Data Retention Regulation*.

93 Artikel 29-gruppens yttrande nr 3/2006 (WP119), rapport 1/2010.

94 Tjeckien, Danmark, Tyskland, Estland, Irland, Grekland, Spanien, Frankrike, Cypern, Lettland, Litauen, Malta, Nederländerna, Österrike, Polen, Slovenien, Slovakien, Finland och Förenade kungariket,

begärdes trots avsaknaden av lagstiftning om införlivande vid denna tidpunkt, samt Tjeckien och Tyskland, vilkas lagar om uppgiftslagring har ogiltigförklarats. Sju medlemsstater som har införlivat direktivet lämnade ingen statistik, även om Belgien lämnade en beräkning av antalet årliga ansökningar av telefoniuppgifter (300 000).

Tillförlitliga kvantitativa och kvalitativa uppgifter är nödvändiga för att påvisa behovet och värdet av säkerhetsåtgärder såsom lagring av uppgifter. Detta erkändes i 2006 års handlingsplan om mätning av brottslighet och straffrättskipning[95], vilken inkluderade ett mål om att utveckla metoder för regelbunden insamling av uppgifter i enlighet med direktivet och att inkludera statistik i Eurostats databas (under förutsättning att de uppfyller kvalitetskraven). Det har inte varit möjligt att uppfylla detta mål, med tanke på att de flesta medlemsstater helt införlivade direktivet först under de två senaste åren och använde sig av olika tolkningar av statistikkällan. Kommissionen kommer i sitt framtida förslag om översyn av ramverket för lagring av uppgifter, tillsammans med översynen av handlingsplanen om statistik, sträva efter att utveckla genomförbara metoder och rapporteringsförfaranden som möjliggör en genomsynlig och meningsfull övervakning av lagring av uppgifter och som inte ger straffrättssystemen och de brottsbekämpande myndigheterna otillbörliga bördor.

4.8. Införlivande i EES-länderna

Island, Liechtenstein och Norge[96] har infört lagstiftning om lagring av uppgifter.

4.9. Beslut från författningsdomstolar om införlivande av lagar

Den rumänska författningsdomstolen ogiltigförklarade i oktober 2009, den tyska federala författningsdomstolen ogiltigförklarade i mars 2010 och den tjeckiska författningsdomstolen ogiltigförklarade i mars 2010 lagarna om införlivande av direktivet i sina respektive jurisdiktioner eftersom de ansågs vara grundlagsstridiga. Den rumänska domstolen[97] accepterade att ett inkräktande på de grundläggande rättigheterna kan tillåtas när det följer vissa regler samt ger lämpliga och tillräckliga skyddsåtgärder mot potentiella godtyckliga åtgärder på myndighetsnivå. Med utgångspunkt från rättspraxis från Europeiska domstolen för de mänskliga rättigheterna[98], fann domstolen att lagen om införlivande var tvetydig i sin tillämpning och sitt syfte med otillräckliga skyddsåtgärder och den framhöll att en "fortlöpande juridisk skyldighet" att lagra alla trafikuppgifter under sex månader var oförenlig med rätten till integritet och yttrandefrihet enligt artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna.

Den tyska författningsdomstolen[99] ansåg att lagring av uppgifter ledde till att den uppfattades som en övervakning som kan hindra det fria utövandet av de grundläggande rättigheterna. Den medgav dock uttryckligen att lagring av uppgifter för strikt begränsad användning tillsammans med tillräckligt hög datasäkerhet inte nödvändigtvis stred mot tysk

---

95 Kommissionens meddelande (2006) 437, *En övergripande och samordnad EU-strategi för mätning av brottslighet och straffrättskipning*: *EU:s handlingsplan 2006–2010*.

96 Lagen om införlivande i Island är lagen om telekommunikationer nr 81/2003 (ändrad i april 2005). I Liechtenstein är det lagen om telekommunikationer från 2006. I Norge godkändes lagen om införlivande den 5 april 2011 och lagen väntar på kunglig promulgation.

97 Rumänska författningsdomstolens beslut nr 1258 av den 8 oktober 2009.

98 Europeiska domstolen för de mänskliga rättigheterna, Rotaru mot Rumänien 2000, Sunday Times mot Förenade kungariket 1979 och Prins Hans-Adam av Liechtenstein mot Rumänien 2001.

99 *Bundesverfassungsgericht, 1 BvR 256/08*, punkt 1–345.

grundlagstiftning. Författningsdomstolen framhöll dock att lagring av dessa uppgifter utgjorde en allvarlig begränsning av rätten till integritet och därför bara borde vara tillåten under synnerligen begränsade omständigheter och att en lagringsperiod på sex månader utgjorde en övre gräns av vad som kunde anses vara proportionerligt (punkt 215). Den ansåg att uppgifter bara bör begäras när det redan föreligger en misstanke om grovt brott eller bevis på en fara för den allmänna säkerheten, och att lagring av uppgifter bör förbjudas vid vissa privilegierade kommunikationer (dvs. sådana som är kopplade till emotionella eller sociala behov) som bygger på konfidentialitet. Uppgifter bör också registreras med en tydlig uppföljning av hur dessa används.

Den tjeckiska författningsdomstolen[100] ogiltigförklarade lagen om införlivande på grundval av att den, som en åtgärd som inkräktade på de grundläggande rättigheterna, inte var tillräckligt bestämd och klar i sin formulering. Domstolen kritiserade ändamålsbegränsningen som otillräckligt avgränsad mot bakgrund av omfattningen och räckvidden på kraven på lagring av uppgifter. Den framhöll att definitionen på de myndigheter som är behöriga att få tillgång till och använda lagrade uppgifter och förfarandena för sådan tillgång och användning inte var tillräckligt tydliga i lagstiftningen om införlivande för att säkerställa uppgifternas integritet och konfidentialitet. Den enskilde medborgaren hade därför otillräckliga garantier och skyddsåtgärder mot offentliga myndigheters eventuella maktmissbruk. Författningsdomstolen kritiserade inte själva direktivet och framhöll att den hade gett tillräckligt utrymme för att Tjeckien skulle kunna införliva det i enlighet med konstitutionen. Författningsdomstolen uttryckte dock i ett *obiter dictum*-uttalande tvivel på nödvändigheten, ändamålsenligheten och lämpligheten i att lagra trafikuppgifter mot bakgrund av att det uppstått nya brottsmetoder, såsom användningen av anonyma SIM-kort.

Dessa tre medlemsstater överväger nu hur man ska återinförliva direktivet. Talan har också väckts i mål som avser lagring i författningsdomstolarna i Bulgarien, vilket lett till en översyn av lagen om införlivande, och i Cypern där de domstolsbeslut som utfärdats enligt lagen om införlivande ansågs vara grundlagsstridiga, och i Ungern där ett mål som gäller underlåtenhet att i lagen om införlivande ange de rättsliga syftena med bearbetningen av uppgifter ännu inte har avgjorts[101].

Kommissionen kommer att överväga de frågeställningar som tagits upp i nationell rättspraxis i sina framtida förslag om översyn av ramverket för lagring av uppgifter.

4.10. Pågående kontroll av efterlevnaden av direktivet

Kommissionen förväntar sig att de medlemsstater som ännu inte helt och fullt har införlivat direktivet, eller som ännu inte antagit lagstiftning som ersätter den lag om införlivande som ogiltigförklarats av de nationella domstolarna, gör det så snart som möjligt. Om detta inte skulle vara fallet förbehåller sig kommissionen rätten att utöva sina befogenheter i enlighet med EU-fördragen. Två medlemsstater som inte har införlivat direktivet (Österrike och Sverige) ansågs av EU-domstolen ha underlåtit att uppfylla sina skyldigheter enligt EU:s

---

100 Tjeckiens författningsdomstols dom av den 22 mars avseende lag nr 127/2005 och dekret nr 485/2005, se punkterna 45–48, 50–51 och 56.

101 Bulagriens högsta förvaltningsdomstol, beslut nr 13627 av den 11 december 2008, Cyperns högsta förvaltningsdomstols överklaganden i målen 65/2009, 78/2009, 82/2009 och 15/2010–22/2010 av den 1 februari 2011, Ungerns talan om fastställelse av oförenlighet med författningen lämnades in av Ungerns *Civil Liberties Union* den 2 juni 2008.

lagstiftning[102]. I april 2011 beslutade kommissionen att en andra gång hänskjuta ärendet avseende Sverige till EU-domstolen för underlåtenhet att uppfylla domen i mål C-185/09 och begärde åläggande av vite enligt artikel 260 i fördraget om Europeiska unionens funktionssätt, efter ett beslut av Sveriges riksdag att under 12 månader uppskjuta antagandet av en lag om införlivande. Kommissionen fortsätter att noggrant följa situationen i Österrike som har lagt fram en tidsplan för att omgående anta en lag om införlivande.

5. DEN ROLL SOM LAGRING AV UPPGIFTER SPELAR VID STRAFFRÄTT OCH BROTTSBEKÄMPNING

I detta avsnitt sammanfattas de funktioner som lagringen av uppgifter har enligt de beskrivningar som medlemsstaterna har lämnat.

5.1. Mängden lagrade uppgifter som de behöriga nationella myndigheterna har tillgång till

Mängden på både teletrafiken och ansökningar om tillgång till trafikuppgifter ökar. Statistik från 19 medlemsstater från endera 2008 och/eller 2009 visar att i hela EU lämnades över 2 miljoner ansökningar om uppgifter varje år, med betydande skillnader mellan medlemsstaterna, från mindre än 100 per år (Cypern) till över 1 miljon (Polen). Enligt information om typen på de begärda uppgifterna från 12 medlemsstater från endera 2008 eller 2009 var de mest ansökta typerna av uppgifter relaterade till mobiltelefoni (se tabellerna 5, 8 och 12). Statistiken anger inte i vilket syfte var och en av ansökningarna lämnades. Tjeckien, Lettland och Polen framhöll att i fallet med uppgifter om mobil telefoni ålades de behöriga myndigheterna att lägga fram samma begäran till var och en av de största mobiltelefonoperatörerna och därför var det faktiska antalet ansökningar per ärende betydligt lägre än vad som framgick av statistiken.

Det finns ingen tydlig förklaring till dessa skillnader, även om befolkningsstorlek, rådande utveckling vad gäller brottslighet, ändamålsbegränsningar och villkor för tillgång och kostnader för att förvärva uppgifter alla är relevanta faktorer.

5.2. Ålder på de lagrade uppgifter som man fått tillgång till

Utifrån den statistiska uppdelning som lämnats av nio medlemsstater[103] för 2008 (se sammanfattningen i tabell 5 och närmare uppgifter i bilagan) var cirka 90 % av de uppgifter som behöriga myndigheter har fått tillgång till under 2008 sex månader gamla eller mindre och cirka 70 % var tre månader gamla eller mindre när (den ursprungliga) ansökan lämnades in.

Tabell 5: Översikt över åldern på de lagrade uppgifter man gett tillgång till i de nio medlemsstater som lämnade en uppdelning av uppgifterna för 2008

Ålder	*Fast telefoni*	*Mobil telefoni*	*Internetuppgifter*	*Sammanlagt*
Mindre än tre månader	61%	70%	56%	67%

[102] Mål C-189/09 respektive C-185/09.

[103] Tjeckien, Danmark, Estland, Irland, Spanien, Cypern, Lettland, Malta och Förenade kungariket.

Tabell 5: Översikt över åldern på de lagrade uppgifter man gett tillgång till i de nio medlemsstater som lämnade en uppdelning av uppgifterna för 2008				
Ålder	*Fast telefoni*	*Mobil telefoni*	*Internetuppgifter*	*Sammanlagt*
3-6 månader	28%	18%	19%	19%
6-12 månader	8%	11%	18%	12%
Över ett år	3%	1%	7%	2%

Enligt majoriteten av medlemsstaterna är användningen av lagrade uppgifter som är äldre än tre och även sex månader mindre vanliga, men kan vara av avgörande betydelse. Användningen av uppgifterna har tenderat att delas upp i tre kategorier. I första hand har internetrelaterade uppgifter tenderat att begäras i ett senare skede än andra former av bevisning under polisutredningar. Analys av uppgifter från telefoni i fasta nät och mobil telefoni genererar ofta potentiella ledtrådar vilka ofta leder till ytterligare ansökningar om äldre uppgifter. Om ett namn under en utredning hittats genom uppgifter från telefoni i fasta nät eller mobil telefoni kan utredarna vilja identifiera den IP-adress (*Internet Protocol*) denna person har använt och kan vilja identifiera vilka den personen har haft kontakt under en given period genom att använda denna IP-adress. I ett sådant scenario kommer utredarna sannolikt att begära uppgifter som gör det möjligt att spåra också kommunikation med andra IP-adresser och identiteten på de personer som har använt dessa IP-adresser.

I andra hand tenderade utredningar av särskilt grova brott, en serie brott, organiserad brottslighet och terroristhandlingar att bygga på äldre lagrade uppgifter som speglar den tid det tar att planera dessa brottsliga gärningar, identifiera kriminella beteendemönster och relationer mellan dem som medverkar i brottet och fastställa den brottsliga avsikten. Verksamhet som kan kopplas till komplicerade ekobrott upptäcks oftast först efter flera månader. I tredje hand, och undantagsvis, har medlemsstaterna begärt trafikuppgifter från en annan medlemsstat, vilken vanligtvis bara kan frigöra dessa uppgifter med rättsligt tillstånd som svar på en framställan om rättsligt bistånd som utfärdats av en domare i den ansökande medlemsstaten. Denna typ av ömsesidigt rättsligt bistånd kan bli en långvarig process, vilken förklarar varför vissa av de begärda uppgifterna var över sex månader gamla.

5.3. Gränsöverskridande ansökningar om lagrade uppgifter

Brottsutredningar och åtal kan inbegripa bevis eller vittnen från, eller händelser som ägde rum i, mer än en medlemsstat. Enligt statistik från medlemsstaterna var mindre än 1 % av alla ansökningar om lagrade uppgifter sådana som hade lagrats i en annan medlemsstat. De brottsbekämpande myndigheterna angav att de föredrar att begära uppgifter från inhemska operatörer, vilka kan ha lagrat de relevanta uppgifterna, än att inleda ömsesidiga rättsliga biståndsförfaranden som kan vara tidskrävande, utan någon garanti om att åtkomst till uppgifterna kommer att beviljas. Rambeslut 2006/960/RIF om ett förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater[104], som anger tidsfrister för tillhandahållande av information efter en ansökan från en annan medlemsstat, är inte tillämpligt, eftersom lagrade uppgifter anses vara information som fåtts genom tvångsåtgärder, vilket ligger utanför instrumentets

[104] Rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater, EUT L 386, 29.12.2006, s. 89 och EUT L 200, 1.8.2007, s. 637.

tillämpningsområde. Ingen medlemsstat eller brottsbekämpande myndighet har dock begärt att detta gränsöverskridande utbyte ska underlättas ytterligare.

5.4. Värdet på lagrade uppgifter i brottsutredningar och åtal

Även om det absoluta antalet ansökningar om uppgifter som rapporteras inte nödvändigtvis speglar uppgifternas värde i enskilda brottsutredningar, rapporterade medlemsstaterna generellt att lagringen av uppgifter åtminstone varit värdefull och i vissa fall oumbärlig[105], för att förhindra och bekämpa brott, inklusive vad gäller skydd av brottsoffer och frikännande av oskyldiga i straffrättsliga förfaranden. Fällande domar bygger på att den dömde förklarar sig vara skyldig, på vittnesmål eller kriminalteknisk bevisning. Det har rapporterats att lagring av trafikuppgifter visat sig vara nödvändig för att kunna kontakta vittnen till en olycka som annars inte skulle ha kunnat identifieras och för att bevisa, eller kunna fastställa, medverkan i brott. Vissa medlemsstater[106] hävdade vidare att lagringen av uppgifter bidragit till att fria personer misstänkta för brott utan att man har behövt ta till andra övervakningsmetoder som skulle ha kunna anses vara mer påträngande.

Det finns ingen allmän definition på *grovt brott* i EU och det finns följaktligen ingen EU-statistik om förekomsten av grov brottslighet eller utredningar eller åtal av grova brott, även om uppgifter om brottslighet och rättsskipning regelbundet offentliggörs. Det sammanlagda antalet ansökningar om lagrade uppgifter som de 19 medlemsstaterna rapporterade från 2009 och/eller 2008 uppgick till cirka 2,6 miljoner. Utifrån den senaste statistiken om brott och straffrättssystem som finns tillgänglig för dessa 19 medlemsstater – vilka avser alla rapporterade brott, inte bara grova brott – kan sägas att det bara förekom något över två ansökningar per polistjänsteman per år, eller ungefär elva ansökningar per 100 rapporterade brott[107].

Utifrån den statistik och de illustrerade exempel som lämnats, vilka länkar användningen av lagrade historiska kommunikationsuppgifter till antalet dömda, frikända, fall som avbrutits och brott som förhindrats, kan ett antal slutsatser dras vad gäller den roll och det värde som lagringen av uppgifter spelar vid brottsutredningar.

Spårning av bevis

I första hand gör lagringen av uppgifter det möjligt att spåra bevis som leder fram till ett brott. Uppgifterna används för att urskilja eller styrka andra former av bevisning när det rör sig om aktiviteter och kopplingar mellan misstänkta. Lokaliseringsuppgifter har särskilt använts, både av brottsbekämpande myndigheter och svaranden, för att utesluta misstänkta personer från brottsplatsen och kontrollera alibin. Denna bevisning kan därför leda till att personer tas bort

---

105 Tjeckien anser lagringen av uppgifter vara helt oumbärlig i ett stort antal ärenden, Ungern anser den vara oumbärlig i [brottsbekämpande myndigheters] regelbundna verksamhet, Slovenien framhåller att avsaknaden av lagrade uppgifter skulle paralysera de brottsbekämpande myndigheternas verksamhet och en brittisk polismyndighet beskriver tillgången på lagrade uppgifter som absolut avgörande för att undersöka terroristhot och grovt brott.

106 Tyskland, Polen, Slovenien och Förenade kungariket.

107 Under 2007 fanns det 1,7 miljoner polistjänstemän i EU-27, av vilka 1,2 miljoner fanns i de 19 medlemsstater som lämnade statistik om ansökningar av lagrade uppgifter. Under 2007 registrerades 29,2 miljoner brott av polisen i EU, av vilka 24 miljoner registrerades i de 19 medlemsstater som lämnade staistik. (Källa: Eurostat 2009).

från polisutredningar och gör att behovet av mer inkräktande undersökningar försvinner, eller leda till frikännanden i en rättegång. Belgien hänvisade till den fällande domen under 2008 mot de gärningsmän som tigerkidnappade en tjänsteman i Antwerpens brottmålsdomstol där lokaliseringsuppgifter kopplade till deras verksamhet i tre olika städer var avgörande för att övertyga juryn om deras medverkan. I ett annat fall, ett mord som begicks 2007 med kopplingar till ett motorcykelgäng, bevisade lokaliseringsuppgifter från förövarnas mobiltelefoner att dessa fanns i området när mordet ägde rum och detta ledde till ett delvist erkännande[108]. Enligt Belgien, Irland och Förenade kungariket kan vissa brott som inbegriper kommunikation genom internet *bara* undersökas genom lagring av uppgifter: t.ex. hot om våld som förmedlas via chattrum lämnar oftast inga andra spår än trafikuppgifter i cyberrymden. En liknande situation gäller i fall av brott som utförs via telefon. Ungern och Polen hänvisade till ett bedrägerifall mot äldre personer under slutet av 2009/början på 2010 som utfördes med hjälp av telefonsamtal där gärningsmännen låtsades vara familjemedlemmar i behov av lån och som bara kunde identifieras genom lagrade telefonuppgifter.

Inledning av brottsutredningar

Det har förekommit fall där det enda sättet att inleda brottsutredningar, i avsaknad av kriminalteknisk bevisning eller ögonvittnesskildringar, har varit att använda lagrade uppgifter. Tyskland lämnade ett exempel på mordet på en polisman där gärningsmannen hade flytt i offrets motorfordon, vilket han sedan övergav. Det var möjligt att fastställa att han därefter använde telefon för att få ett alternativt transportmedel. Det fanns ingen kriminalteknisk bevisning eller ögonvittnesbevisning för att identifiera mördaren och myndigheterna var beroende av tillgången till dessa trafikuppgifter för att kunna fullfölja utredningen. I fall med internetrelaterade sexuella övergrepp mot barn har lagringen av uppgifter varit nödvändig för en lyckad utredning. Tillsammans med andra undersökningstekniker ger lagring av uppgifter det möjligt att identifiera konsumenter av barnpornografiskt innehåll[109] och stödja identifiering och undsättning av barn som är offer. Tjeckien rapporterade att utan tillgång till lagrade internetuppgifter skulle det ha varit omöjligt att inleda utredningar som ett led i "operation Vilma" i ett nät av användare och spridare av barnpornografi. På EU-nivå har ändamålet med operation Rescue (som leds genom Europol) för att skydda barn mot missbruk hindrats på grund av att avsaknaden av lagstiftning om införlivande av lagring av uppgifter har hindrat vissa medlemsstater från att undersöka medlemmar i ett omfattande internationellt pedofilnät som använder IP-adresser, vilka kan vara upp till ett år gamla.

Vid utredning av cyberbrottslighet är en IP-adress oftast det första spåret. Vid brottsbekämpning kan man genom att hämta trafikuppgifter identifiera abonnenten av IP-adressen innan man bestämmer om en brottsutredning kan inledas. Polisen kan därmed också ges möjlighet att förvarna potentiella offer om cyberattacker. När polisen lyckas beslagta en server som botnetoperatörer använder som ledningssystem kan den bara se de IP-adresser som

---

108 *National Policing Improvement Agency (UK), The Journal of Homicide and Major Incident Investigation*, Volume 5, Issue 1, våren 2009, s. 39–51.

109 Projektet *Measurement and analysis of p2p activity against paedophile content*, som stödjs genom programmet säkrare internet, gav korrekt information om pedofilers verksamhet i systemet *eDonkey peer-to-peer*, vilket gjorde det möjligt att identifiera 178 000 användare (av 89 miljoner undersökta användare) som begärde pedofilinnehåll.

är kopplade till den servern, men genom att få tillgång till lagrade uppgifter kan polisen identifiera och varna de potentiella offer som äger dessa IP-adresser.

Lagrade uppgifter är en integrerad del av brottsutredningar

Även om brottsbekämpande myndigheter och domstolar i de flesta medlemsstater inte för statistik över vilken typ av bevis som visade sig vara avgörande för att säkerställa fällande domar eller frikännanden ingår lagringen av uppgifter till fullo i utredning och åtal i EU. Vissa medlemsstater menade att de inte alltid kunde påvisa vilken inverkan lagrade uppgifter hade på resultatet på brottsutredningar och åtal, eftersom domstolarna överväger all bevisning som presenteras för den och sällan anser att ett enda bevis är avgörande[110]. Nederländerna rapporterade att mellan januari och juli 2010 hade historiska trafikuppgifter varit en avgörande faktor i 24 domstolsavgöranden. Finland rapporterade att i 56 % av de 3 405 ansökningarna visade sig lagrade uppgifter endera vara viktiga eller avgörande för att upptäcka och/eller åtala brott. Förenade kungariket lämnade uppgifter för att försöka kvantifiera den inverkan som lagringen av uppgifter hade på åtal för brott, och rapporterade att för tre av dess brottsbekämpande organ användes lagrade uppgifter i merparten av eller vid alla utredningar som ledde till straffrättsliga förfaranden och straffrättsliga påföljder.

5.5. Teknisk utveckling och användningen av förbetalda SIM-kort

Brottsbekämpningen måste hålla samma steg som den tekniska utveckling som används för att begå eller medverka till brott. Lagringen av uppgifter ingår i de redskap som är nödvändiga vid brottsutredning för att rusta de brottsbekämpande myndigheterna att på ett hanterbart och kostnadseffektivt sätt hantera den nutida brottsutvecklingens mångfald, volym och hastighet. Ett antal kommunikationsformer som ökar allt mer ligger utanför direktivets tillämpningsområde. Virtuella privata nät i exempelvis universitet eller stora bolag ger flera användare tillgång till internet via en enda nätport med samma IP-adress. Ny teknik som gör det möjligt att förse individuella VPN-användare med adresser håller på att införas.

Andelen mobiltelefonanvändare som använder sig av förbetalda tjänster varierar i EU. Vissa medlemsstater har hävdat att anonyma förbetalda SIM-kort, särskilt när de köpts i en annan medlemsstat, också kan användas av personer som är inblandade i brottslig verksamhet som ett sätt att undvika identifiering vid brottsutredningar[111]. Sex medlemsstater (Danmark, Spanien, Italien, Grekland, Slovakien och Bulgarien) har antagit åtgärder som kräver registrering av förbetalda SIM-kort. Dessa och andra medlemsstater (Polen, Cypern, Litauen) har argumenterat för att en åtgärd ska införas på EU-nivå om obligatorisk registrering av identiteten på användare av förbetalda tjänster. Inga bevis har lämnats vad gäller dessa nationella åtgärders effektivitet. Potentiella begränsningar har belysts, t.ex. i fall med identitetsstöld eller när ett SIM-kort köps av en tredje part eller en användare ”roamar” med ett kort som köpts i ett tredjeland. På det hela taget är inte kommissionen övertygad om behovet av att i detta skede vidta åtgärder på detta område på EU-nivå.

---

110 Belgien, Tjeckien, Litauen.

111 Rådets slutsatser om kampen mot brottsligt missbruk och anonym användning av elektronisk kommunikation.

6. INVERKAN AV LAGRINGEN AV UPPGIFTER PÅ OPERATÖRER OCH KONSUMENTER

6.1. Operatörer och konsumenter

I ett gemensamt uttalande till kommissionen har fem stora branschsammanslutningar förklarat att direktivets ekonomiska inverkan var betydande eller enorm för mindre tjänsteleverantörer, eftersom direktivet lämnar ett stort manöverutrymme[112]. Åtta operatörer lämnade mycket varierande beräkningar av kostnaderna för kapital och driftsutgifter för efterlevnaden av direktivet. Detta kan bekräftas genom de indikationer av nivån på ersättningen av operatörernas kostnader som fyra medlemsstater rapporterat (se tabell 6).

I en undersökning som genomfördes innan direktivet införlivades i merparten av medlemsstaterna beräknades kostnaderna för att införa ett system för lagring av uppgifter för en leverantör av internettjänster som betjänade 500 000 kunder till cirka 375 240 euro under det första året och 9 870 euro i driftskostnader per månad därefter,[113] och kostnaderna för att inrätta ett system för lagring av uppgifter till 131 190 euro, med driftskostnader på 28 960 euro per månad. Den tyska författningsdomstolen fann i sin dom av den 2 mars 2010 att avgiften för lagring inte var överdriven för de berörda tjänsteleverantörerna eller oproportionerlig i förhållande till de ekonomiska bördor som ålades företagen till följd av lagringsavgiften[114]. Kostnaden för lagring av uppgifter per enhet står i ett omvänt förhållande till operatörens storlek och den standardiseringsnivå en medlemsstat antagit för samverkan med operatörerna[115].

De flesta operatörer framhöll i sina svar på kommissionens frågeformulär att de inte kunde ange direktivets inverkan på konkurrensen, detaljhandelspriser för konsumenterna eller investeringar i ny infrastruktur eller tjänster.

Det finns inga bevis på att direktivet haft några kvantifierbara eller väsentliga effekter på konsumentpriserna för elektroniska kommunikationstjänster. Företrädarna för konsumenterna bidrog inte till 2009 års offentliga samråd. En undersökning som utfördes i Tyskland för en medborgarrättsorganisation tydde på att konsumenterna hade för avsikt att ändra sina kommunikationsvanor och undvika att använda elektroniska kommunikationstjänster under vissa omständigheter; det finns dock inga bestyrkande bevis på att någon ändring av vanorna skulle ha ägt rum i någon berörd medlemsstat eller i EU i allmänhet[116].

Kommissionen har för avsikt att bedöma vilken inverkan framtida ändringar av direktivet kan få på näringslivet och kunderna eventuellt genom en särskild Eurobarometerundersökning för att bedöma allmänhetens inställning.

---

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF.

113 Wilfried Gansterer & Michael Ilger, Lagring av uppgifter – EU:s direktiv 2006/24/EG ur ett tekniskt perspektiv, Wien: *Verlag Medien und Recht*, 2008.

114 *Bundesverfassungsgericht, 1 BvR* 256/08 av den 2 mars 2010, punkt 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx.

116 Undersökningen utfördes av Forsa och beställdes av AK Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

6.2. Ersättning av kostnader

I direktivet regleras inte ersättningen av de kostnader som uppstår för operatörerna till följd av kravet på lagring av uppgifter. Dessa kostnader består av:

1.11. *Driftskostnader* som avser kostnader eller återkommande utgifter som är kopplade till verksamhetens drift, en anordning, komponent, del av utrustning eller anläggning.

1.12. *Kapitalkostnader* som avser utgifter som skapar framtida fördelar eller kostnader för att utveckla eller tillhandahålla delar som inte är förbrukningsbara för produkten eller systemet, vilka kan inkludera kostnaderna för arbetstagare och sådana kostnader som hyra och allmännyttiga tjänster.

Samtliga medlemsstater garanterar någon form av ersättning om uppgifterna begärs i samband med ett brottsmålsförande i domstol. Två medlemsstater rapporterade att de ersätter både driftskostnader och kapitalkostnader. Sex medlemsstater ersätter bara driftskostnader. Inget annat ersättningssystem har anmälts till kommissionen. Närmare uppgifter finns i tabell 6.

Tabell 6: Medlemsstater som ersätter kostnader

Medlemsstat	**Driftskostnader**	**Kapitalkostnader**	**Årliga ersättningskostnader (miljoner euro)**
Belgien	Ja	Nej	22 (2008)
Bulgarien	Nej	Nej	-
Tjeckien	Inte införlivat[117].		
Danmark	Ja	Nej	-
Tyskland	Inte införlivat.		
Estland	Ja	Nej	-
Irland	Nej	Nej	-
Grekland	Nej	Nej	-
Spanien	Nej	Nej	-
Frankrike	Ja	Nej	-
Italien	-	-	-
Cypern	Nej	Nej	-
Lettland	Nej	Nej	-
Litauen	Ja, om de begärs och är berättigade.	Nej	-
Luxemburg	Nej	Nej	-
Ungern	Nej	Nej	-
Malta	Nej	Nej	-
Nederländerna	Ja	Nej	-
Österrike	Inte införlivat.		
Polen	Nej	Nej	-
Portugal	Nej	Nej	-
Rumänien	Inte införlivat.		
Slovenien	Nej	Nej	-

[117] Innan Tjeckiens lag om införlivande ogiltigförklarades ersatte Tjeckien både driftskostnader och kapitalkostnader och redovisade under 2009 ersättningskostnader på 6,8 miljoner euro.

Slovakien	Nej	Nej	-
Finland	Ja	Ja	1
Sverige	Inte införlivat.		
Förenade kungariket	Ja	Ja	55 miljoner euro (har ersatts sammanlagt för kostnader som uppstått under tre år).

Av vad som framgår ovan kan slutsatsen dras att direktivet inte helt uppfyllt sitt mål vad gäller att införa likvärdiga förutsättningar för operatörerna i EU. Kommissionen kommer att överväga alternativen för att minimera hindren för en fungerande inre marknad genom att säkerställa att operatörerna konsekvent ersätts för de kostnader de ådrar sig för att uppfylla kraven om lagring av uppgifter, där små och medelstora operatörer särskilt bör uppmärksammas.

7. LAGRINGENS INVERKAN PÅ DE GRUNDLÄGGANDE RÄTTIGHETERNA

7.1. Grundläggande rättigheter till integritet och skydd av personuppgifter

Lagring av uppgifter utgör en begränsning av rätten till privatliv och skydd av personuppgifter, vilka är grundläggande rättigheter i EU[118]. Denna begränsning ska enligt artikel 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter. Detta innebär i praktiken att alla begränsningar ska[119]

1.13. formuleras på ett tydligt och förutsägbart sätt,

1.14. vara nödvändiga för att nå ett mål av allmänt intresse eller för att skydda andras rättigheter och friheter,

1.15. vara proportionerliga i förhållande till det avsedda målet, och

1.16. bevara det väsentliga innehållet i de grundläggande rättigheter som berörs.

I artikel 8.2 i Europakonventionen om skydd för de mänskliga rättigheterna medges också att en offentlig myndighets ingripande i en persons rätt till integritet kan motiveras som nödvändigt för att säkerställa nationell säkerhet, allmän säkerhet eller för att förhindra

---

118 Artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (EUT C 83, 30.3.2010, s. 389) garanterar var och en rätten till ”skydd av de personuppgifter som rör honom eller henne.” Artikel 16 i fördraget om Europeiska unionens funktionssätt (EUT C 83, 30.3.2010, s. 1) garanterar var och en rätten till ”skydd av de personuppgifter som rör honom eller henne.”

119 Se kommissionens checklista över grundläggande rättigheter avseende alla lagstiftningsförslag i kommissionens meddelande KOM (2010) 573/4, *Strategi för Europeiska unionens konkreta tillämpning av stadgan om de grundläggande rättigheterna.*

brott[120]. I artikel 15.1 i direktiv 2002/58/EG och skälen i direktiv 2006/24/EG upprepas dessa principer, vilka ligger till grund för EU:s inställning till lagring av uppgifter.

Genom rättspraxis i EU-domstolen och Europeiska domstolen för de mänskliga rättigheterna har villkor utvecklats avseende de begränsningar som rätten till integritet måste uppfylla. Dessa domar är av relevans för om direktivet ska ändras, särskilt vad gäller villkoren för tillgång till och användning av lagrade uppgifter.

Eventuella begränsningar av rätten till integritet ska vara exakta och förutsägbara

I målet Österreichischer Rundfunk framhöll EU-domstolen att eventuell interferens i lag avseende rätten till integritet ska formuleras med tillräcklig exakthet för att ge medborgaren möjlighet att anpassa sitt beteende i enlighet därmed… [för att uppfylla] kraven på förutsägbarhet.

Eventuella begränsningar av rätten till integritet måste vara nödvändig med minimigarantier

I målet Copland mot Förenade kungariket som gällde statens övervakning av telefonsamtal, e-postmeddelanden och internetanvändning framhöll Europeiska domstolen för mänskliga rättigheter att en sådan begränsning av rätten till integritet bara kunde anses vara nödvändig om den baserades på relevant nationell lagstiftning[121]. I målet S. and Marper mot Förenade kungariket som gällde lagring av DNA-profiler eller fingeravryck av personer som frikänts från brott eller vars åtal lagts ned innan en eventuell fällande dom, framhöll domstolen att en sådan begränsning av rätten till integritet bara kunde motiveras om den uppfyllde ett pressande socialt behov, om den stod i proportion till ändamålet med den och om de skäl som lagts fram av den offentliga myndigheten för att motivera den var relevant och tillräcklig[122]. Enligt huvudprinciperna för uppgiftsskydd ska lagringen av uppgifter stå i proportion till ändamålet med insamlingen och lagringstiden vara begränsad[123]. För telefonavlyssning, hemlig övervakning och insamling av underrättelser är det väsentligt att ha tydliga och detaljerade regler avseende åtgärdernas tillämpning och tillämpningsområde samt minimigarantier för bland annat varaktighet, lagring, användning, tillgång för tredje parter, förfaranden för att bevara uppgifternas och förfarandenas integritet och konfidentialitet när de ska förstöras, vilka ger tillräckliga garantier mot risken för missbruk och godtycklighet.

Eventuella begränsningar av rätten till integritet måste stå i proportion till allmänintresset

EU-domstolen fann i sin dom i målet Schecke & Eifert avseende offentliggörandet av alla mottagare av jordbrukssubventioner på internet[124] att det inte verkade som om EU i sin lagstiftning hade vidtagit lämpliga åtgärder för att uppnå balans när det gäller respekten för de centrala aspekterna i rätten till integritet och det allmänna intresset (insyn) som erkänts i EU.

---

120 Artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (ETS nr 5), Europarådet, 4.11.1950.

121 Copland mot Förenade kungariket, dom i Europeiska domstolen för mänskliga rättigheter, Strasbourg, 3.4.2007, s. 9.

122 Marper mot Förenade kungariket, dom i Europeiska domstolen för mänskliga rättigheter, Strasbourg, 4.12.2008, s. 31.

123 Marper, s. 30.

124 C-92/09 Volker och Markus Schecke GbR mot Land Hessen och C-93/09 Eifert mot Land Hessen och Bundesanstalt für Landwirtschaft und Ernährung, 9.11.10.

Domstolen ansåg att lagstiftarna inte hade övervägt några andra metoder som skulle ha stämt överens med målet samtidigt som det inkräktade mindre på rättigheterna för mottagarna av subventioner att respektera deras privatliv och skydda deras personuppgifter. Domstolen framhöll att lagstiftarna hade överskridit proportionalitetsgränserna, eftersom begränsningarna i förhållande till skyddet av personuppgifter bara ska tillämpas i den utsträckning de är absolut nödvändiga.

7.2. Kritik av principen om lagring av uppgifter

Ett flertal medborgarrättsgrupper har skrivit till kommissionen och hävdat att lagring av uppgifter i princip är en omotiverad och onödig begränsning av individernas rätt till integritet. De anser den icke-konventionella generella och godtyckliga lagringen av individers telekomtrafik-, lokaliserings- och abonnentuppgifter vara en olaglig begränsning av de grundläggande rättigheterna. Efter att ett ärende hänskjutits till domstol i en medlemsstat (Irland) av en medborgarrättsgrupp förväntas frågan om direktivets laglighet hänskjutas till Europeiska unionens domstol[125]. Också den europeiska datatillsynsmannen uttryckte tvivel om behovet av åtgärden.

7.3. Uppmaning till stärkta regler om uppgiftsskydd och datasäkerhet

I artikel 29-gruppens rapport om den andra brottsbekämpningsåtgärden fanns argument om att riskerna för brott mot integritet vid kommunikationer och yttrandefrihet och informationsfrihet fanns inbyggda i lagringen av alla trafikuppgifter. Den kritiserade vissa aspekter i det nationella genomförandet, särskilt loggning, lagringsperioder, den typ av uppgifter som lagrades och datasäkerhetsåtgärder. Arbetsgruppen rapporterade fall där detaljer om *innehållet* i internetrelaterade kommunikationer, som låg utanför direktivets tillämpningsområde, lagrades, inklusive IP-adresser och URL-adresser till webbplatser, rubriker på e-postmeddelanden och förteckningen över mottagare i fältet ”kopia till”. Den begärde därför ett klargörande om att kategorierna skulle vara uttömmande och att inga ytterligare skyldigheter om lagring av uppgifter skulle åläggas operatörerna.

Europeiska datatillsynsmannen hävdar att direktivet har misslyckats med att harmonisera nationell lagstiftning och att användningen av lagrade uppgifter inte är begränsad till att bekämpa grov brottslighet[126]. Han framhåller att ett EU-instrument som innehåller regler om obligatorisk lagring av uppgifter också, om ett behov skulle uppstå, bör innehålla regler om tillgång till uppgifter för brottsbekämpning och fortsatt användning. Han har uppmanat EU att anta omfattande lagstiftning som inte bara ålägger operatörerna att lagra uppgifter, utan också reglerar hur medlemsstaterna ska använda uppgifterna i brottsbekämpningssyfte för att skapa ”rättssäkerhet för medborgarna”.

Myndigheter med ansvar för skydd av uppgifter har argumenterat att lagringen i sig själv innebär en risk för potentiella överträdelser av integriteten, vilka inte hanteras på EU-nivå i direktivet, utan istället kräver att medlemsstaterna ska säkerställa att de nationella reglerna för skydd av uppgifter respekteras. Även om det inte finns några konkreta exempel på allvarliga brott mot integriteten kvarstår risken för brott mot uppgiftsskydd och den kan komma att växa i takt med teknikens utveckling och trender i olika kommunikationer, oavsett om uppgifterna

---

125 Den 5 maj 2010 beviljade *Irish High Court* ett yrkande till *Digital Rights Ireland Limited* för ett hänskjutande till EU-domstolen enligt artikel 267 i fördraget om Europeiska unionens funktionssätt.

126 Tal av Peter Hustinx på konferensen *Taking on the Data Retention Directive* den 3 december 2010.

lagras för kommersiella eller säkerhetsmässiga ändamål, inom eller utanför EU, om inte ytterligare säkerhetsåtgärder vidtas.

8. SAMMANFATTNING OCH REKOMMENDATIONER

I denna rapport belyses ett antal fördelar i det nuvarande systemet för lagring av uppgifter och de områden som kan förbättras. EU antog direktivet vid en tidpunkt där risken för ett överhängande hot för terroristattacker var högt. Den konsekvensbedömning som kommissionen avser att genomföra ger möjlighet att bedöma lagringen av uppgifter i EU och pröva om den uppfyller kraven i nödvändighets- och proportionalitetstesten och med hänsyn till de inre säkerhetsintressena, den inre marknadens smidiga funktion och för att stärka respekten för privatlivet och den grundläggande rätten till skydd av personuppgifter. Kommissionens förslag om översyn av ramen för lagring av uppgifter bör bygga på följande slutsatser och rekommendationer.

8.1. EU bör stödja och reglera lagringen av uppgifter som en nödvändig säkerhetsåtgärd

Merparten av medlemsstaterna anser att EU:s regler om lagring av uppgifter är nödvändiga som ett redskap för brottsbekämpning, skydd av brottsoffer och straffrättssystemen. De bevis i form av statistik och exempel som medlemsstaterna lämnat är begränsade i vissa avseenden men pekar inte desto mindre på den mycket viktiga roll som lagringen av uppgifter spelar vid brottsutredningar. Dessa uppgifter ger värdefulla ledtrådar och bevis vid förebyggande och åtal av brott och säkerställande av straffrättsskipning. Användningen av uppgifterna har lett till fällande domar vid straffbara gärningar vilka, utan lagring, kanske aldrig skulle ha lösts. Lagringen har också lett till att oskyldiga personer har kunnat frikännas. Harmoniserade regler på området säkerställer att lagringen av uppgifter är ändamålsenlig vid bekämpningen av brott, att näringslivet ges rättssäkerhet om en väl fungerande inre marknad och att de höga nivåerna av respekt för integritet och skydd av personuppgifter tillämpas konsekvent inom hela EU.

8.2. Införlivandet har varit ojämnt

Införlivande lagstiftningen är i kraft i 22 medlemsstater. Det betydande utrymme som lämnats åt medlemsstaterna för att anta åtgärder om lagring av uppgifter enligt artikel 15.1 i direktiv 2002/58/EG gör bedömningen av direktiv 2006/24/EG högst problematisk. Det förekommer betydande skillnader mellan införlivandet av lagstiftning på områdena ändamålsbegränsning, tillgång till uppgifter, lagringsperioder, uppgiftsskydd och datasäkerhet samt statistik. Tre medlemsstater har begått överträdelser av direktivet sedan deras lagstiftning om införlivande ogiltigförklarades av deras respektive författningsdomstolar. Två andra medlemsstater har ännu inte genomfört det. Kommissionen kommer att fortsätta att arbeta med alla medlemsstater för att bidra till att säkerställa ett effektivt genomförande av direktivet. Den kommer också att fortsätta att spela sin roll vad gäller att genomföra EU-lagstiftning och i sista hand, om så krävs, tillämpa överträdelseförfaranden.

8.3. Direktivet har inte fullt ut harmoniserat synen på lagringen av uppgifter eller skapat likvärdiga konkurrensvillkor för operatörer

Direktivet har säkerställt att lagring av uppgifter nu genomförs i de flesta medlemsstaterna. Direktivet garanterar inte i sig självt att uppgifterna lagras, hämtas och används helt i enlighet

med rätten till integritet och skydd av personuppgifter. Medlemsstaterna har ansvar för att säkerställa att dessa rättigheter upprätthålls. Direktivet strävade bara efter en delvis harmonisering av synen på lagring av uppgifter. Det är därför ingen överraskning att det inte finns någon gemensam metod, vare sig vad gäller särskilda bestämmelser i direktivet, som ändamålsbegränsning eller lagringsperioder, eller aspekter som ligger utanför tillämpningsområdet, som ersättning av kostnader. Utöver den variationsgrad som uttryckligen föreskrivs i direktivet har skillnaderna i den nationella tillämpningen av lagringen av uppgifter visat sig medföra stora svårigheter för operatörerna.

8.4. Operatörerna bör konsekvent ersättas för de kostnader de ådrar sig

Avsaknaden av rättssäkerhet för näringslivet fortsätter. Skyldigheten att lagra och hämta uppgifter utgör en betydande kostnad för operatörerna, särskilt mindre operatörer, och operatörerna påverkas och ersätts på olika sätt i vissa medlemsstater jämfört med andra, även om det inte finns några bevis på att telekomsektorn i sin helhet har påverkats negativt till följd av direktivet. Kommissionen kommer att överväga hur operatörerna konsekvent kan erhålla ersättning.

8.5. Säkerställa proportionalitet vid den helautomatiska hanteringen av lagring, hämtning och användning

Kommissionen kommer att säkerställa att eventuella framtida förslag om lagring av uppgifter respekterar principen om proportionalitet och är lämplig för att uppnå målet att bekämpa grova brott och terrorism och inte sträcker sig längre än vad som är nödvändigt för att uppnå detta. Den kommer att erkänna att eventuella undantag eller begränsningar vad gäller skyddet av personuppgifter bara ska tillämpas i den utsträckning dessa är nödvändiga. Den kommer att noga överväga inverkan på effektivitet och ändamålsenlighet när det gäller straffrättssystemet och brottsbekämpningen, för integritet och kostnader för offentlig administration och operatörer, strängare bestämmelser vad gäller lagring, tillgång till och användning av trafikuppgifter. Följande områden bör särskilt undersökas vid konsekvensbedömningen:

1. En konsekvent begränsning av ändamålet med lagringen av uppgifter och typer av brott där lagrade uppgifter kan hämtas och användas.

2. Ökad harmonisering av och en möjlig förkortning av de obligatoriska lagringsperioderna.

3. Säkerställa oberoende övervakning av ansökningarna om tillgång, de lagrade uppgifterna och de bestämmelser om tillgång som är tillämpliga på alla medlemsstaterna.

4. Begränsa de myndigheter som är behöriga att få tillgång till uppgifterna.

5. Minska de kategorier av uppgifter som ska lagras.

6. Ge riktlinjer för tekniska och organisationsmässiga säkerhetsåtgärder för tillgång till uppgifter inklusive överlämnanderutiner.

7. Ge riktlinjer för användningen av uppgifter inklusive för att hindra datautvinning.

8. Utveckla genomförbara metoder och rapporteringsförfaranden för att underlätta jämförelser vid tillämpning och utvärdering av ett framtida instrument.

Kommissionen kommer också att överväga om, och om så är fallet, hur en metod för frysning av uppgifter på EU-nivå kan komplettera lagringen.

Med hänvisning till checklistan över de grundläggande rättigheterna och förhållningssättet vad gäller hantering av information på området frihet, säkerhet och rättvisa[127] kommer kommissionen att överväga vart och ett av dessa områden i enlighet med principerna om proportionalitet och kravet på förutsägbarhet. Den kommer också att säkerställa överensstämmelse med den pågående översynen av EU:s lagstiftning avseende skyddet av personuppgifter[128].

8.6. Kommande åtgärder

Mot bakgrund av denna utvärdering kommer kommissionen att föreslå en översyn av nuvarande ramverk för lagring av uppgifter. Den kommer att tänka ut ett antal alternativ i samråd med brottsbekämpande myndigheter, rättsväsendet, näringslivet och konsumentgrupper, datatillsynsmyndigheter och medborgarrättsgrupper. Den kommer att undersöka allmänhetens uppfattning om lagring av uppgifter och dess inverkan på beteende och vanor. Resultaten av dessa undersökningar kommer att ingå i en konsekvensbedömning av de strategiska alternativ som identifierats och utgöra en grund för kommissionens förslag.

---

127 Se hänvisningen ovan till meddelandet om tillämpningen av stadgan om de grundläggande rättigheterna: *Översikt av informationshanteringen inom området med frihet, säkerhet och rättvisa*, KOM(2010)385, 20.7.2010.

128 KOM(2010) 609, 4.11.2010.

Bilaga: Ytterligare statistik avseende lagringen av trafikuppgifter

Noter till bilagan:

1. Med uppgifternas ålder avses den tid som förflutit från det datum då uppgifterna lagrades och det datum då den behöriga myndigheten begärde att uppgifterna skulle överföras.

2. Internetrelaterade uppgifter omfattar uppgifter som avser internetåtkomst, internetbaserad e-post och internettelefoni.

3. Statistik för Tjeckien, Lettland och Polen som omfattas av förbehåll (se avsnitt 5.1).

Statistik som medlemsstaterna lämnat för 2008

Tabell 7: Ansökningar om lagrade trafikuppgifter efter ålder 2008									
Ålder på de begärda uppgifterna (månader)/medlemsstat:	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totalt**
Belgien	Inga.								
Bulgarien	Inga.								
Tjeckien	102691	18440	10110	319	0	0	0	0	131560
Danmark	2669	672	185	37	23	2	7	4	3599
Tyskland	9363	2336	985	0	0	0	0	0	12684
Estland	2773	733	157	827	0	0	0	0	4490
Irland	8981	2016	936	1855	90	85	78	54	14095
Grekland	Ingen uppdelning efter ålder.								584
Spanien	22629	15868	10298	4783	0	0	0	0	53578
Frankrike	Ingen uppdelning efter ålder.								**503437**
Italien	Inga.								
Cypern	30	4	0	0	0	0	0	0	34
Lettland	10539	2739	1368	1211	597	438	0	0	16892
Litauen	55735	23817	5251	512	0	0	0	0	85315
Luxemburg	Inga.								
Ungern	Inga.								
Malta	810	59	0	0	0	0	0	0	869
Nederländerna	Ingen uppdelning efter ålder.								85000
Österrike	Ingen uppdelning efter ålder.								3093
Polen	Inga.								
Portugal	Inga.								
Rumänien	Inga.								
Slovenien	Ingen uppdelning efter ålder.								2821
Slovakien	Inga.								
Finland	9134	1144	448	214	268				4008
Sverige	Inga.								
Förenade kungariket	315350	88339	34665	19398	6385	2973	1536	1576	470222
Totalt	**533504**	**156167**	**64403**	**29156**	**7095***	**3230***	**1353***	**1366***	**1392281**

* Utom Finland.

Tabell 8: Ansökningar om lagrade trafikuppgifter efter typ 2008 (Anges inom parentes i de fall där ansökningar om uppgifter inte kunde beviljas – om uppgifter lämnats)				
Typ av uppgift/ medlemsstat	**Fast telefonnät**	**Mobil telefoni**	**Internettelefoni**	**Totalt**
Belgien	Inga.			
Bulgarien	Inga.			
Tjeckien	**4983 (131)**	**125040 (2276)**	**1537 (83)**	**131560 (2490)**
Danmark	**192 (0)**	**3273 (5)**	**134 (0)**	**3599 (5)**
Tyskland	Ingen uppdelning efter ålder.			**12684 (931)**
Estland	**4114 (1519)**	**376 (7)**	**Inga.**	**4490 (1526)**
Irland	**5317 (16)**	**5873 (48)**	**2905 (33)**	**14095 (97)**
Grekland	Ingen uppdelning efter ålder.			**584**
Spanien	**4448 (0)**	**40013 (0)**	**9117 (0)**	**53578 (0)**
Frankrike	Ingen uppdelning efter ålder.			**503437**
Italien	Inga.			
Cypern	**3 (0)**	**31 (5)**	**0 (0)**	**34 (5)**
Lettland	**1602 (90)**	**14238 (530)**	**1052 (76)**	**16892 (696)**
Litauen	**765 (72)**	**84550 (5657)**	**Inga.**	**85315 (5729)**
Luxemburg	Inga.			
Ungern	Inga.			
Malta	**29 (0)**	**748 (120)**	**92 (13)**	**869 (133)**
Nederländerna	Ingen uppdelning efter ålder.			**85000**
Österrike	Ingen uppdelning efter ålder.			**3093**
Polen	Inga.			
Portugal	Inga.			
Rumänien	Inga.			
Slovenien	Ingen uppdelning efter ålder.			**2821**
Slovakien	Inga.			
Finland	Ingen uppdelning efter ålder.			**4008**
Sverige	Inga.			
Förenade kungariket	**90747 (0)**	**329421 (0)**	**50054 (0)**	**470222 (0)**
Totalt				**1392281**

Tabell 9: Ansökningar om lagrade trafikuppgifter från *fasta telefonnät* som överförts 2008, indelade efter ålder									
Ålder på de begärda uppgifterna (månader)/medlemsstat:	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totalt**
Belgien	Inga.								
Bulgarien	Inga.								
Tjeckien	3669	916	143	124	0	0	0	0	4852
Danmark	133	28	31	0	0	0	0	0	192
Tyskland	Inga.								
Estland	1876	161	74	484	0	0	0	0	2595
Irland	4118	712	197	182	32	21	23	16	5301
Grekland	Inga.								
Spanien	1948	1431	741	328	0	0	0	0	4448
Frankrike	Inga.								
Italien	Inga.								
Cypern	3	0	0	0	0	0	0	0	3
Lettland	698	213	167	193	104	137	0	0	1512
Litauen	251	442	0	0	0	0	0	0	693
Luxemburg	Inga.								
Ungern	Inga.								
Malta	28	1	0	0	0	0	0	0	29
Nederländerna	Inga.								
Österrike	Inga.								
Polen	Inga.								
Portugal	Inga.								
Rumänien	Inga.								
Slovenien	Inga.								
Slovakien	Inga.								
Finland	Inga.								
Sverige	Inga.								
Förenade kungariket	54805	27052	5340	753	1135	437	1050	175	90747
Totalt	**67529**	**30956**	**6693**	**2064**	**1271**	**595**	**1073**	**191**	**110372**

Tabell 10: Ansökningar om lagrade trafikuppgifter från *mobil telefoni* som överförts 2008, indelade efter ålder									
Ålder på de begärda uppgifterna (månader)/medlemsstat:	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totalt**
Belgien	Inga.								
Bulgarien	Inga.								
Tjeckien	98232	17013	7518	1	0	0	0	0	122764
Danmark	2433	628	143	33	20	1	7	3	3268
Tyskland	Inga.								
Estland	248	58	35	28	0	0	0	0	369
Irland	4326	820	230	240	57	63	52	37	5825
Grekland	Inga.								
Spanien	17403	12114	7444	3052	0	0	0	0	40013
Frankrike	Inga.								
Italien	Inga.								
Cypern	23	3	0	0	0	0	0	0	26
Lettland	8928	2298	1085	746	394	257	0	0	13708
Litauen	55484	23375	14	20	0	0	0	0	78893
Luxemburg	Inga.								
Ungern	Inga.								
Malta	575	53	0	0	0	0	0	0	628
Nederländerna	Inga.								
Österrike	Inga.								
Polen	Inga.								
Portugal	Inga.								
Rumänien	Inga.								
Slovenien	Inga.								
Slovakien	Inga.								
Finland	Inga.								
Sverige	Inga.								
Förenade kungariket	229375	52241	26228	16040	3333	521	339	1344	329421
Totalt	**417027**	**108603**	**42697**	**20160**	**3804**	**842**	**398**	**1384**	**594915**

Tabell 11: Ansökningar om lagrade trafikuppgifter från *internet* som överförts 2008, indelade efter ålder									
Ålder på de begärda uppgifterna (månader)/medlemsstat:	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totalt**
Belgien	Inga.								
Bulgarien	Inga.								
Tjeckien	737	412	137	168	0	0	0	0	1454
Danmark	102	14	11	2	3	1	0	1	134
Tyskland	Inga.								
Estland	Inga.								
Irland	492	460	498	1422	0	0	0	0	2872
Grekland	Inga.								
Spanien	3278	2323	2113	1403	0	0	0	0	9117
Frankrike	Inga.								
Italien	Inga.								
Cypern	0	0	0	0	0	0	0	0	0
Lettland	424	150	75	219	74	34	0	0	976
Litauen	Inga.								
Luxemburg	Inga.								
Ungern	Inga.								
Malta	76	3	0	0	0	0	0	0	79
Nederländerna	Inga.								
Österrike	Inga.								
Polen	Inga.								
Portugal	Inga.								
Rumänien	Inga.								
Slovenien	Inga.								
Slovakien	Inga.								
Finland	Inga.								
Sverige	Inga.								
Förenade kungariket	31170	9046	3097	2605	1917	2015	147	57	50054
Totalt	**36279**	**12408**	**5931**	**5819**	**1994**	**2050**	**147**	**58**	**64686**

Statistik som medlemsstaterna lämnat för 2009

Tabell 12: Ansökningar om lagrade uppgifter efter ålder 2009									
Ålder på de begärda uppgifterna (månader)/medlemsstat:	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totalt**
Belgien	Inga.								
Bulgarien	Inga.								
Tjeckien	210975	56623	11620	1053	0	0	0	0	280271
Danmark	2980	685	179	104	54	38	12	14	4066
Tyskland	Inga.								
Estland	4299	1836	1210	1065	0	0	0	0	8410
Irland	8117	1652	805	297	168	134	69	41	11283
Grekland	Inga.								
Spanien	29775	19346	13999	6970	0	0	0	0	70090
Frankrike	Ingen uppdelning efter ålder.								514813
Italien	Inga.								
Cypern	31	8	1	0	0	0	0	0	40
Lettland	20758	2414	1088	796	565	475	0	0	26096
Litauen	30247	35456	5886	884	0	0	0	0	72473
Luxemburg	Inga.								
Ungern	Inga.								
Malta	3336	362	151	174	0	0	0	0	4023
Nederländerna	Inga.								
Österrike	Inga.								
Portugal	Inga.								
Rumänien	Inga.								
Polen	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Slovenien	Ingen uppdelning efter ålder.								1918
Slovakien	Ingen uppdelning efter ålder.								5214
Finland	2000	1310	532	152	76	0	0	0	4070
Sverige	Inga.								
Förenade kungariket	Inga.								
Totalt	**954845**	**297998**	**110996**	**64021**	**27961**	**24571**	**14065**	**34683**	**2051085**

Tabell 13: Ansökningar om lagrade uppgifter efter typ 2009 (Anges inom parentes i de fall där ansökningar om uppgifter inte kunde beviljas – om dessa lämnats)				
Typ av uppgift/ medlemsstat	**Fast telefonnät**	**Mobil telefoni**	**Internettelefoni**	**Totalt**
Belgien	Inga.			
Bulgarien	Inga.			
Tjeckien	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Danmark	133 (0)	3771 (10)	162 (1)	4066 (11)
Tyskland	Inga.			
Estland	6422 (2279)	902 (21)	1086 (468)	8410 (2768)
Irland	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Grekland	Inga.			
Spanien	5055 (0)	56133 (0)	8902 (0)	70090 (0)
Frankrike	Ingen uppdelning efter ålder.			**514813**
Italien	Inga.			
Cypern	0 (0)	23 (3)	14 (0)	40 (3)
Lettland	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Litauen	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Luxemburg	Inga.			
Ungern	Inga.			
Malta	156 (10)	3693 (882)	174 (10)	4023 (902)
Nederländerna	Inga.			
Österrike	Inga.			
Polen	Ingen uppdelning efter ålder.			**1048318**
Portugal	Inga.			
Rumänien	Inga.			
Slovenien	Ingen uppdelning efter ålder.			**1918 (48)**
Slovakien	Ingen uppdelning efter ålder.			**5214 (157)**
Finland	Ingen uppdelning efter ålder.			**4070**
Sverige	Inga.			
Förenade kungariket	Inga.			
Totalt				**2051082 (1069885)**

Tabell 14: Ansökningar om lagrade uppgifter från *fasta telefonnät* som överförts 2009, indelade efter ålder									
Ålder på de begärda uppgifterna (månader)/medlemsstat:	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totalt**
Belgien	Inga.								
Bulgarien	Inga.								
Tjeckien	9919	2907	47	36	0	0	0	0	12909
Danmark	105	19	7	2	0	0	0	0	133
Tyskland	Inga.								
Estland	2254	866	599	424	0	0	0	0	4143
Irland	3934	337	69	70	50	39	16	11	4526
Grekland	Inga.								
Spanien	2371	1492	844	348	0	0	0	0	5055
Frankrike	Inga.								
Italien	Inga.								
Cypern	0	0	0	0	0	0	0	0	0
Lettland	744	253	157	143	68	89	0	0	1454
Litauen	469	773	73	6	0	0	0	0	1321
Luxemburg	Inga.								
Ungern	Inga.								
Malta	83	25	18	20	0	0	0	0	146
Nederländerna	Inga.								
Österrike	Inga.								
Polen	Inga.								
Portugal	Inga.								
Rumänien	Inga.								
Slovenien	Inga.								
Slovakien	Inga.								
Finland	Inga.								
Sverige	Inga.								
Förenade kungariket	Inga.								
Totalt	**19879**	**6672**	**1814**	**1049**	**118**	**128**	**16**	**11**	**29687**

Tabell 15: Ansökningar om lagrade uppgifter från *mobil telefoni* som överförts 2009, indelade efter ålder									
Ålder på de begärda uppgifterna (månader)/medlemsstat:	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totalt**
Belgien	Inga.								
Bulgarien	Inga.								
Tjeckien	197620	48841	472	0	0	0	0	0	246933
Danmark	2777	639	162	98	47	19	12	7	3761
Tyskland	Inga.								
Estland	318	397	96	70	0	0	0	0	881
Irland	3669	835	220	210	115	92	50	28	5219
Grekland	Inga.								
Spanien	24065	15648	11147	5273	0	0	0	0	56133
Frankrike	Inga.								
Italien	Inga.								
Cypern	17	16	0	0	0	0	0	0	23
Lettland	18832	1912	778	515	394	263	0	0	22694
Litauen	25713	19595	28	0	0	0	0	0	45336
Luxemburg	Inga.								
Ungern	Inga.								
Malta	2332	246	111	122	0	0	0	0	2811
Nederländerna	Inga.								
Österrike	Inga.								
Polen	Inga.								
Portugal	Inga.								
Rumänien	Inga.								
Slovenien	Inga.								
Slovakien	Inga.								
Finland	Inga.								
Sverige	Inga.								
Förenade kungariket	Inga.								
Totalt	**275343**	**88119**	**13014**	**6288**	**556**	**374**	**62**	**35**	**383791**

Tabell 16: Ansökningar om lagrade uppgifter från *internet* som överförts 2009, indelade efter ålder									
Ålder på de begärda uppgifterna (månader)/medlemsstat:	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Totalt**
Belgien	Inga.								
Bulgarien	Inga.								
Tjeckien	3369	4811	861	942	0	0	0	0	9983
Danmark	98	27	10	4	4	7	0	1	151
Tyskland	Inga.								
Estland	315	145	56	102	0	0	0	0	618
Irland	489	455	502	0	0	0	0	0	1446
Grekland	Inga.								
Spanien	3339	2206	2008	1349	0	0	0	0	8902
Frankrike	Inga.								
Italien	Inga.								
Cypern	12	2	0	0	0	0	0	0	14
Lettland	852	198	74	90	88	86	0	0	1388
Litauen	4060	15087	1	88	0	0	0	0	19236
Luxemburg	Inga.								
Ungern	Inga.								
Malta	150	14	0	0	0	0	0	0	164
Nederländerna	Inga.								
Österrike	Inga.								
Polen	Inga.								
Portugal	Inga.								
Rumänien	Inga.								
Slovenien	Inga.								
Slovakien	Inga.								
Finland	Inga.								
Sverige	Inga.								
Förenade kungariket	Inga.								
Totalt	**12684**	**22945**	**3512**	**2575**	**92**	**93**	**0**	**1**	**41902**