I

(Resolutioner, rekommendationer och yttranden)

YTTRANDEN

EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen om förslaget till Europaparlamentets och rådets direktiv om ändring av bland annat direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)

(2008/C 181/01)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE,

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

med beaktande av 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 ([1]),

med beaktande Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation ([2]),

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, särskilt artikel 41 ([3]),

med beaktande av begäran om ett yttrande enligt artikel 28.2 i förordning (EG) nr 45/2001, inkommen den 16 november 2007 från Europeiska kommissionen.

HÄRIGENOM FRAMFÖRS FÖLJANDE:

I **INLEDNING**

1. Den 13 november 2007 antog kommissionen ett förslag till direktiv om ändring av bland annat direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (nedan kallat ”förslaget” eller ”de föreslagna ändringarna”). Den för närvarande gällande versionen av direktiv 2002/58/EG benämns vanligtvis, och så även i detta yttrande, direktivet om integritet och elektronisk kommunikation.

([1]) EGT L 281, 23.11.1995, s. 31.
([2]) EGT L 201, 31.7.2002, s. 37.
([3]) EGT L 8, 12.1.2001, s. 1.

2. Förslaget syftar till att förbättra skyddet för enskilda personer med avseende på integritet och behandling av personuppgifter inom sektorn för elektronisk kommunikation. Detta sker inte genom att man helt och hållet omstöper det befintliga direktivet om integritet och elektronisk kommunikation, utan i stället genom att man föreslår specifika ändringar i det, vilka huvudsakligen syftar till att förstärka de säkerhetsrelaterade bestämmelserna och förbättra genomförandemekanismerna.

3. Förslaget ingår i en vidare reform som gäller EU:s fem direktiv om telekommunikation ("telekompaketet"). Utöver förslagen till översyn av telekompaketet ([1]) har kommissionen samtidigt även antagit ett förslag till förordning om inrättande av en europeisk myndighet för marknaden för elektronisk kommunikation ([2]).

4. Synpunkterna i detta yttrande begränsar sig till de föreslagna ändringarna av direktivet om integritet och elektronisk kommunikation såvida inte dessa bygger på begrepp eller bestämmelser i förslagen till översyn av telekompaketet. Dessutom gäller vissa synpunkter i detta yttrande bestämmelser i direktivet om integritet och elektronisk kommunikation, som inte ändras genom förslaget.

5. Detta yttrande tar upp följande ämnesområden: *i)* räckvidden för direktivet om integritet och elektronisk kommunikation, i synnerhet berörda tjänster (föreslagen ändring av artikel 3.1), *ii)* obligatoriska anmälningar av säkerhetsöverträdelser (föreslagen ändring genom vilken artikel 4.3 och 4.4 införs), *iii)* bestämmelserna om kakor, spionvara och liknande anordningar (föreslagen ändring av artikel 5.3), *iv)* de rättsliga åtgärder som vidtas av leverantörer av elektroniska kommunikationstjänster och andra juridiska personer (föreslagen ändring genom vilken artikel 13.6 införs) samt *v)* skärpta bestämmelser om genomförandet (föreslagen ändring genom vilken artikel 15a införs).

Samråd med Europeiska datatillsynsmannen och bredare offentligt samråd

6. Kommissionen översände förslaget till Europeiska datatillsynsmannen den 16 november 2007. Europeiska datatillsynsmannen uppfattar detta meddelande som en begäran om att lämna rekommendationer till gemenskapsinstitutionerna och gemenskapsorganen i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (nedan kallad *förordning (EG) nr 45/2001*).

7. Före antagandet av förslaget samrådde kommissionen informellt med Europeiska datatillsynsmannen om utkastet till förslag, vilket Europeiska datatillsynsmannen välkomnade eftersom det gav honom tillfälle att lämna vissa förslag på utkastet till förslag innan detta antogs av kommissionen. Europeiska datatillsynsmannen gläder sig över att några av hans förslag har tagits upp i förslaget.

8. Antagandet av förslaget föregicks av ett brett offentligt samråd, ett förfarande som Europeiska datatillsynsmannen har värdesatt. I juni 2006 inledde kommissionen ett offentligt samråd om dess meddelande om översyn av telekompaketet, där kommissionen redovisade sina synpunkter på läget och lade fram vissa förslag till ändringar ([3]). Artikel 29-gruppen för skydd av personuppgifter ("artikel 29-gruppen"), i vilken Europeiska datatillsynsmannen är medlem, utnyttjade detta tillfälle till att lämna sina synpunkter på de föreslagna ändringarna i ett yttrande som antogs den 26 september 2006 ([4]).

([1]) De föreslagna ändringarna i telekomdirektiven läggs fram i följande förslag: *i)* Förslag till Europaparlamentets och rådets direktiv om ändring av direktiv 2002/21/EG om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/19/EG om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter och direktiv 2002/20/EG om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster, 13.11.2007, KOM(2007) 697 slutlig, samt *ii)* Förslag till Europaparlamentets och rådets direktiv om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om konsumentskyddssamarbete, 13.11.2007, KOM(2007) 698 slutlig.

([2]) Förslag till Europaparlamentets och rådets förordning om inrättande av en europeisk myndighet för marknaden för elektronisk kommunikation, 13.11.2007, KOM(2007) 699 slutlig.

([3]) Meddelande om EU:s regelverk för elektroniska kommunikationsnät och kommunikationstjänster (SEK(2006) 816), antaget den 29 juni 2006. Meddelandet vidareutvecklades genom ett arbetsdokument från kommissionen (KOM(206) 334 slutlig).

([4]) Yttrande 8/2006 om översynen av regelverket för elektroniska meddelanden och tjänster, med inriktning på direktivet om integritet och elektronisk kommunikation, antaget den 26 september 2006.

Europeiska datatillsynsmannens allmänna synpunkter

9. På det hela taget är Europeiska datatillsynsmannens synpunkter i fråga om förslaget positiva. Europeiska datatillsynsmannen stöder till fullo kommissionens syften med att anta ett förslag för att förstärka skyddet av människors integritet och personuppgifter inom sektorn för elektronisk kommunikation. Europeiska datatillsynsmannen välkomnar särskilt beslutet om att införa ett system för obligatoriska anmälningar av säkerhetsöverträdelser (ändring av artikel 4 i direktivet om integritet och elektronisk kommunikation, genom vilken punkterna 3 och 4 läggs till). Om databrott inträffar finns det klara nyttoeffekter med anmälan, eftersom en sådan förstärker organisationers ansvarighet, är en faktor som förmår företagen att införa strikta säkerhetsåtgärder och möjliggör fastställande av tillförlitligaste teknik för att skydda uppgifter. Dessutom ger den de drabbade en möjlighet att vidta åtgärder för att skydda sig mot identitetsstöld eller annat missbruk av deras personuppgifter.

10. Europeiska datatillsynsmannen välkomnar andra ändringar i förslaget som att juridiska personer med legitima intressen får vidta rättsliga åtgärder mot personer som överträder vissa av bestämmelserna i direktivet om integritet och elektronisk kommunikation (ändring av artikel 13 genom tillägg av punkt 6). Positivt är även förstärkandet av de nationella tillsynsmyndigheternas undersökande befogenheter, eftersom detta kommer att göra det möjligt för dessa att bedöma om en uppgiftsbehandling har utförts i enlighet med lagen samt att avslöja överträdare (tillägget av artikel 15a.3). För att så snabbt som möjligt kunna stoppa olaglig behandling av personuppgifter och integritetsintrång behövs det en åtgärd för att skydda människors fri- och rättigheter. Därför välkomnas i hög grad den föreslagna artikel 15a.2, i vilken man erkänner de nationella tillsynsmyndigheternas befogenhet att kräva att överträdelser upphör, eftersom den kommer att ge dessa myndigheter möjlighet att omedelbart stoppa grovt olaglig uppgiftsbehandling.

11. Inriktningen i förslaget samt flertalet föreslagna ändringar ligger i linje med de synpunkter i fråga om den framtida dataskyddspolitiken som redovisats i tidigare yttranden från Europeiska datatillsynsmannen, som yttrandet om genomförandet av dataskyddsdirektivet ([1]). Inställningen grundar sig bland annat på uppfattningen att det inte behövs några nya principer för dataskyddet, men att det behövs mer specificerade regler för att gripa sig an de frågor gällande uppgiftsskydd som ställs på grund av ny teknik, som Internet, RFID osv., samt redskap som hjälper till att genomföra och effektivisera dataskyddslagstiftningen, som att man ger juridiska personer möjlighet att vidta rättsliga åtgärder mot kränkande av uppgiftsskyddet och ålägger de dataregisteransvariga att anmäla säkerhetsöverträdelser.

12. Trots den övergripande positiva inriktningen i förslaget beklagar Europeiska datatillsynsmannen att detta inte är så ambitiöst som det hade kunnat vara. Sedan 2003 har genomförandet av bestämmelserna i direktivet om integritet och elektronisk kommunikation samt en noggrant utförd analys av ämnet visat att vissa av dess bestämmelser är långt ifrån klara och tydliga, vilket ger upphov till rättslig osäkerhet och problem i fråga om efterlevnaden. Detta är till exempel fallet i fråga om i vilken utsträckning halvstatliga leverantörer av elektroniska kommunikationstjänster omfattas av direktivet om integritet och elektronisk kommunikation. Man hade hoppats att kommissionen skulle ha utnyttjat översynen av telekompaketet, och i synnerhet av direktivet om integritet och elektronisk kommunikation, till att lösa visa kvarstående problem. Vad gäller nya frågor, som inrättandet av ett system för obligatoriska anmälningar av säkerhetsöverträdelser, erbjuder man genom förslaget endast en partiell lösning som inte inom räckvidden för de organisationer som är skyldiga att anmäla säkerhetsöverträdelser inbegriper enheter som behandlar ytterst känsliga slag av uppgifter som Internetbanker eller leverantörer av hälso- och sjukvård via Internet. Europeiska datatillsynsmannen beklagar denna uppläggning.

13. Europeiska datatillsynsmannen hyser förhoppning om att de lagstiftande organen när förslaget passerar genom lagstiftningsförfarandet kommer att beakta synpunkterna och förslagen i detta yttrande för att lösa de frågor som inte tagits upp i kommissionens förslag.

([1]) Yttrande från Europeiska datatillsynsmannen av den 25 juli 2007 om meddelandet från kommissionen till Europaparlamentet och rådet om uppföljningen av arbetsprogrammet för ett bättre genomförande av dataskyddsdirektivet, EUT C 255, 27.10.2007, s. 1.

II ANALYS AV FÖRSLAGET

II.1 Räckvidden för direktivet om integritet och elektronisk kommunikation, i synnerhet berörda tjänster

14. En central fråga i det nuvarande direktivet om integritet och elektronisk kommunikation är frågan om dess tillämpningsområde. Förslaget innehåller vissa positiva inslag som definierar och förtydligar dess räckvidd, framför allt i fråga om de tjänster som berörs av direktivet, vilket tas upp nedan i avsnitt i. Tyvärr löser man genom de föreslagna ändringarna inte alla befintliga problem. Som det tas upp i avsnitt ii nedan söker man tyvärr inte att genom ändringarna utvidga tillämpningsområdet för direktivet till att även omfatta elektroniska kommunikationstjänster via privata nät.

15. I artikel 3 i direktivet om integritet och elektronisk kommunikation anges de tjänster som berörs av direktivet, med andra ord de tjänster i fråga om vilka de skyldigheter som anges i direktivet ska tillämpas, på följande sätt: ”Detta direktiv ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät”.

16. Således är de tjänster som berörs av direktivet om integritet och elektronisk kommunikation leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät. Definitionen av leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät ges i ramdirektivet ([1]). Allmänna kommunikationsnät definieras i artikel 2 d i ramdirektivet ([2]). I den verksamhet som utövas av leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät ingår tillhandahållande av Internetanslutning, överföring av information via elektroniska nät, mobil- och telefonförbindelser m.m.

i) *Föreslagen ändring av artikel 3 i direktivet om integritet och elektronisk kommunikation: de berörda tjänsterna ska inbegripa allmänna kommunikationsnät som stöder datainsamling och identifikationsutrustning*

17. I förslaget ändras artikel 3 i direktivet om integritet och elektronisk kommunikation genom att man anger att allmänna elektroniska kommunikationsnät ska inbegripa ”allmänna kommunikationsnät som stöder datainsamling och identifikationsutrustning”. I skäl 28 förklaras att utvecklingen av tillämpningar som medför datainsamling, inbegripet av personuppgifter, och använder radiofrekvenser, som RFID, ska omfattas av direktivet om integritet och elektronisk kommunikation, om dessa är sammankopplade med eller använder allmänna kommunikationsnät eller -tjänster.

18. Europeiska datatillsynsmannen finner denna bestämmelse positiv, eftersom den förtydligar att ett antal RFID-tillämpningar ligger inom tillämpningsområdet för direktivet om integritet och elektronisk kommunikation och därigenom undanröjer viss osäkerhet på denna punkt och slutgiltigt undanröjer missförstånd och feltolkningar av lagen.

19. Enligt den nuvarande artikel 3 i direktivet om integritet och elektronisk kommunikation omfattas redan vissa RFID-tillämpningar av direktivet. Detta har flera kumulativa skäl. För det första eftersom RFID-tillämpningar faller under definitionen av elektroniska kommunikationstjänster. För det andra eftersom de tillhandahålls via ett elektroniskt kommunikationsnät, om tillämpningarna stöds av ett överföringssystem som trådlöst överför signaler. Slutligen kan nätet vara antingen allmänt eller privat.

([1]) Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (EGT L 108, 24.4.2002, s. 33). I ramdirektivet avgränsar man vad som avses med elektronisk kommunikationstjänst på följande sätt: i) En *elektronisk kommunikationstjänst* är en tjänst som vanligen tillhandahålls mot ersättning och som utgörs av överföring av signaler i nät, däribland teletjänster och överföringstjänster i nät. ii) Tjänster som tillhandahåller innehåll som överförts med hjälp av elektroniska kommunikationsnät och elektroniska tjänster är undantagna i definitionen av elektronisk kommunikationstjänst. iii) Med tillhandahållande av tjänster avses etablering, drift, kontroll eller tillgängliggörande av ett nät. iv) Elektroniska kommunikationstjänster omfattar inte informationssamhällets tjänster, som i direktivet om elektronisk handel definieras som tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare.

([2]) Med allmänt kommunikationsnät avses ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster.

Om det är allmänt kommer RFID-tillämpningar att betraktas som ”berörda tjänster” och därmed ligga inom tillämpningsområdet för direktivet om integritet och elektronisk kommunikation. Genom den föreslagna ändringen kommer man dock att undanröja alla kvarstående tvivel härom och därigenom sörja för ett klarare rättsläge.

20. Som det framhållits i ett tidigare yttrande från Europeiska datatillsynsmannen om RFID ([1]) utesluter självfallet inte denna bestämmelse ett eventuellt behov av att anta ytterligare rättsliga instrument för RFID. Dock bör sådana åtgärder beslutas i ett annat sammanhang och inte ingå i förslaget.

ii) *Behovet av att inbegripa elektroniska kommunikationstjänster via privata eller halvprivata nät*

21. Europeiska datatillsynsmannen välkomnar det ovan angivna förtydligandet men beklagar att man i förslaget inte har tagit sig an den allt mer otydliga åtskillnaden mellan privata och allmänna nät. Vidare beklagar Europeiska datatillsynsmannen att definitionen av de tjänster som omfattas av direktivet om integritet och elektronisk kommunikation inte har utvidgats till att även omfatta privata nät. I sin nuvarande lydelse gäller artikel 3.1 i direktivet om integritet och elektronisk kommunikation endast *elektroniska kommunikationstjänster via allmänna nät*.

22. Europeiska datatillsynsmannen noterar att tendensen till att tjänster i ökad utsträckning blir blandat privata och offentliga. Exempel på detta är universitet som möjliggör för tusentals studenter att använda Internet och e-post. Det är uppenbart att dessa halvoffentliga (eller halvprivata) nät kan inkräkta på enskildas integritet, och detta påkallar därför att man bör låta detta slag av tjänster omfattas av samma regler som de som gäller för rent allmänna nät. Dessutom har privata nät, som sådana genom vilka arbetsgivare tillhandahåller de anställda tillgång till Internet samt hotell- och lägenhetsägare telefon och e-post till sina gäster liksom Internetkaféer, en inverkan på uppgiftsskyddet och integriteten för nyttjarna, vilket ger vid handen att även de bör täckas in i tillämpningsområdet för direktivet om integritet och elektronisk kommunikation.

23. Rättspraxis i vissa medlemsstater har också redan ålagt elektroniska kommunikationstjänster som tillhandahålls via privata nät samma skyldigheter som de som de som tillhandahålls via allmänna nät ([2]). Även enligt tysk lag har dataskyddsmyndigheter funnit att ett tillåtande att använda privat e-post inom ett företag kan medföra att företaget betraktas som operatör i fråga om offentliga telekommunikationstjänster och därigenom omfattas av bestämmelserna i direktivet om integritet och elektronisk kommunikation.

24. Kort sagt motiverar den ökande betydelsen av de blandade (privata/allmänna) och privata näten i vardagslivet, med i konsekvens därmed ökande risk för personuppgifter och integritet, att man behöver tillämpa samma regler för dessa tjänster som dem som gäller för offentliga elektroniska kommunikationstjänster. Därför anser Europeiska datatillsynsmannen att direktivet bör ändras för att utvidga tillämpningsområdet till att även omfatta sådana privata tjänster, en åsikt som delas av artikel 29-gruppen ([3]).

II.2 **Obligatoriska anmälningar av säkerhetsöverträdelser: ändring av artikel 4**

25. Artikel 4 i direktivet om integritet och elektronisk kommunikation ändras genom att man inför två nya punkter (3 och 4), i vilka det anges en skyldighet att anmäla säkerhetsöverträdelser. Enligt artikel 4.3 åläggs leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät dels att till de nationella tillsynsmyndigheterna utan onödiga dröjsmål anmäla varje säkerhetsöverträdelse som leder till en oavsiktlig eller olaglig förstörelse, förlust, ändring eller ett inte auktoriserat avslöjande av eller tillgång till personuppgifter som överförts, lagrats eller på annat sätt behandlats i samband med tillhandahållandet av allmänna kommunikationstjänster (sammantaget ”äventyrande av uppgifter”), dels också att anmäla detta till sina kunder.

([1]) Yttrande av den 20 december 2007 om meddelandet från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén ”Radiofrekvensidentifiering (RFID) i Europa: på väg mot en strategi”, KOM(2007) 96.

([2]) Exempelvis fann appellationsdomstolen i Paris i sin dom i målet *BNP Paribas* mot *World Press Online*, avkunnad den 4 februari 2005, att det inte förelåg någon skillnad mellan Internetleverantörer som erbjuder Internettillgång kommersiellt och arbetsgivare som ger sina anställda tillgång till Internet.

([3]) Yttrande 8/2006 om översynen av regelverket för elektroniska meddelanden och tjänster, med inriktning på direktivet om integritet och elektronisk kommunikation, antaget den 26 september 2006.

Nyttoeffekterna av denna skyldighet

26. Europeiska datatillsynsmannen välkomnar dessa bestämmelser (artikel 4.3 och 4.4) genom vilka man inför obligatorisk anmälan av säkerhetsöverträdelser. Anmälan av säkerhetsöverträdelser medför positiva effekter för skyddet för personuppgifter och integritet, vilket redan har prövats i Förenta staterna, där det på delstatsnivå har funnits en lagstiftning om anmälan av överträdelser i flera år.

27. För det första ökar en lagstiftning om anmälan av överträdelser ansvarigheten för leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät i fråga om den information som har äventyrats. Inom ramen för uppgiftsskyddet eller integritetspolitiken innebär ansvarighet att varje organisation är ansvarig för den information som befinner sig under dess uppsikt och kontroll. Anmälningsskyldigheten innebär dels en bekräftelse av att de uppgifter som har äventyrats befann sig under kontroll av leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät, dels att det är denna organisations ansvar att vidta nödvändiga åtgärder gentemot sådana uppgifter.

28. För det andra har förekomsten av anmälningar av säkerhetsöverträdelser visat sig vara en faktor som driver fram säkerhetsinvesteringar inom organisationer som behandlar personuppgifter. Det enkla förhållandet att man måste anmäla säkerhetsöverträdelser föranleder organisationer att införa striktare säkerhetsnormer som skyddar personuppgifter och förhindrar överträdelser. Dessutom kommer anmälningar om säkerhetsöverträdelser att bidra till att man ringar in och genomför en tillförlitlig statistisk analys av de effektivaste lösningarna och mekanismerna i fråga om säkerheten. Det har under en lång tid rått brist på hårddata om brister i datasäkerheten samt om den lämpligaste tekniken för att skydda uppgifter. Detta problem kommer sannolikt att lösas genom skyldighet att anmäla säkerhetsöverträdelser, såsom fallet var med de amerikanska lagarna om rapportering av säkerhetsöverträdelser, eftersom anmälningar kommer att ge information om vilken teknik som mest gynnar överträdelser ([1]).

29. Slutligen gör anmälningar av säkerhetsöverträdelser enskilda personer medvetna om de risker de löper när deras personuppgifter äventyras och hjälper dem att vidta de åtgärder som behövs för att mildra sådana risker. Exempelvis kan, om bankuppgifter har äventyrats, den som är informerad besluta att ändra uppgifterna för åtkomst till sitt bankkonto för att hindra någon från att bemäktiga sig dessa uppgifter och använda dem i olagligt syfte (vanligen kallat ”identitetsstöld”). Sammanfattningsvis minskar nämnda skyldighet sannolikenheten för att enskilda ska utsättas för identitetsstöld, och den kan också hjälpa offer att vidta de åtgärder som behövs för att lösa olika problem.

Brister i den föreslagna ändringen

30. Europeiska datatillsynsmannen är nöjd med det system med anmälan av säkerhetsöverträdelser som anges i bestämmelserna i artikel 4.3 och 4.4 men skulle önska att de tillämpas i vidare omfattning så att de inbegriper leverantörer av informationssamhällets tjänster. Detta skulle innebära att även Internetbanker, Internetföretag, leverantörer av hälso- och sjukvård via Internet osv. omfattas av lagen ([2]).

31. De skäl som motiverar att man ålägger leverantörer av offentliga elektroniska kommunikationstjänster en skyldighet att anmäla säkerhetsöverträdelser föreligger även i fråga om andra organisationer som också behandlar mycket stora mängder personuppgifter, vilka om de avslöjas kan vara särskilt negativa för registrerade personer. Detta inbegriper Internetbanker och datamäklare samt andra Internetleverantörer som behandlar känsliga uppgifter (vilket inbegriper hälsouppgifter, politiska åsikter m.m.). Äventyrande av information som innehas av Internetbanker och Internetföretag, vilken kan innefatta inte endast bankkontonummer utan även kreditkortsuppgifter, kan utlösa identitetsstöld, varvid det är av grundläggande betydelse att människor uppmärksammas så att de kan vidta de åtgärder som behövs. I det senare fallet (hälso- och sjukvård via Internet) kommer människor förvisso att riskera att lida, om inte ekonomisk skada, så dock icke ekonomisk skada när känsliga uppgifter äventyras.

([1]) Se rapporten ”*Security Economics and the Internal Market*” av professorerna Ross Anderson, Rainer Böhme, Richard Clayton och Tyler Moore, beställd av Europeiska byrån för nät- och informationssäkerhet. Rapporten finns tillgänglig på http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Leverantörer av informationssamhällets tjänster definieras i direktivet om elektronisk handel som tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare.

32. Genom en utvidgning av räckvidden för denna skyldighet kommer dessutom de ovan angivna nyttoeffekter som förväntas genom åläggandet av denna skyldighet inte att begränsas till en verksamhetssektor, nämligen leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster, utan kommer att utvidgas till att omfatta informationssamhällets tjänster i allmänhet. Att man ålägger informationssamhällets tjänster som Internetbanker en skyldighet att anmäla säkerhetsöverträdelser kommer förvisso inte endast att öka deras ansvarighet, utan det kommer även att motivera dessa aktörer att förstärka sina säkerhetsåtgärder och därigenom undvika eventuella framtida säkerhetsöverträdelser.

33. Det finns andra precedensfall där direktivet om integritet och elektronisk kommunikation redan gäller andra enheter än leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät, som artikel 5 om konfidentialitet vid kommunikation och artikel 13 om skräppost. Detta bekräftar att de lagstiftande organen tidigare mycket klokt har beslutat att utvidga räckvidden för vissa bestämmelser i direktivet om integritet och elektronisk kommunikation, eftersom de fann detta lämpligt och nödvändigt. Europeiska datatillsynsmannen hoppas att de lagstiftande organen nu inte kommer att tveka inför att inta en liknande förnuftig och flexibel hållning och utvidga räckvidden för artikel 4 till att även omfatta leverantörer av informationssamhällets tjänster. För detta skulle det räcka att i artikel 4.3 införa ett omnämnande av leverantörerna av informationssamhällets tjänster, enligt följande: ”Vid en säkerhetsöverträdelse, som leder till en oavsiktlig eller (…) ska leverantören av allmänt tillgängliga elektroniska kommunikationstjänster och leverantören av informationssamhällets tjänster (…) meddela den berörda abonnenten och den berörda nationella tillsynsmyndigheten denna överträdelse”.

34. Europeiska datatillsynsmannen ser att denna bestämmelse och dess tillämpning på både leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät och leverantörer av informationssamhällets tjänster som ett första steg i en utveckling som slutligen kan tillämpas på samtliga dataregisteransvariga.

Särskild rättslig ram för säkerhetsöverträdelser genom ett kommittéförfarande

35. Förslaget tar inte upp ett antal frågor rörande skyldigheten att anmäla säkerhetsöverträdelser. Exempel på frågor som behöver tas upp är omständigheterna för underrättelsen samt tillämplig form och tillämpligt förfarande. I stället låter man genom artikel 4.4 i förslaget dessa beslut antas genom ett kommittéförfarande ([1]), nämligen genom den kommunikationskommitté som inrättas genom artikel 22 i ramdirektivet, i enlighet med rådets beslut av den 28 juni 1999. Närmare bestämt kommer åtgärderna att antas i enlighet med artikel 5 i rådets beslut av den 28 juni 1999, genom vilket man inför regler för det föreskrivande förfarandet i fråga om ”åtgärder med allmän räckvidd som är avsedda att tillämpa bestämmelser som utgör del av de viktigaste grunddragen i grundläggande rättsakter”.

36. Europeiska datatillsynsmannen motsätter sig inte att man överlåter samtliga dessa frågor till genomförandelagstiftningen. Antagande av lagstiftning via ett kommittéförfarande kan sannolikt förkorta lagstiftningsförfarandet. Kommittéförfarandet kommer också att bidra till att säkerställa harmonisering, vilket är ett eftersträvansvärt mål.

37. Med tanke på det stora antal frågor som kommer att behöva tas upp i genomförandebestämmelserna och den betydelse som dessa har, vilket belyses i det nedanstående, förefaller det lämpligt att man tar sig an dem alla i en enda lagstiftning och inte som ett lapptäcke, varvid vissa frågor skulle tas upp i direktivet om integritet och elektronisk kommunikation och andra överlåtas till genomförandelagstiftningen. Därför bör man välkomna kommissionens uppläggning som går ut på att man överlåter dessa beslut till genomförandelagstiftningen och till att antas efter samråd med Europeiska datatillsynsmannen, samt förhoppningsvis med andra berörda parter (se nästa punkt).

Frågor som behöver tas upp via genomförandebestämmelser

38. Betydelsen av genomförandebestämmelserna belyses om man med någon detaljrikedom anger de frågor som kommer att behöva tas upp i dessa. Genom genomförandebestämmelser kan man fastställa de standarder enligt vilka underrättelsen ska lämnas. Exempelvis kommer man i dessa att ange vad som utgör en säkerhetsöverträdelse, de villkor under vilka underrättelser till enskilda och myndigheterna ska lämnas samt tidsramarna för underrättelsen och anmälan.

([1]) Lagstiftningsförfarande inom EG som innefattar kommittéer sammansatta av företrädare för medlemsstaternas regeringar på tjänstemannanivå.

39. Europeiska datatillsynsmannen anser att direktivet om integritet och elektronisk kommunikation, och framför allt artikel 4, inte bör innehålla några undantag från skyldigheten att göra anmälan. I detta hänseende gläder sig Europeiska datatillsynsmannen över kommissionens modell i artikel 4, genom vilken det anges en skyldighet att anmäla och inte anges något undantag från detta, utan genom vilken man överlåter denna och andra frågor som behöver tas upp till genomförandelagstiftningen. Europeiska datatillsynsmannen är medveten om argument som kan motivera vissa undantag från skyldigheten men förordar att man omsorgsfullt tar upp dessa frågor i genomförandelagstiftningen, efter en ingående och övergripande diskussion av samtliga aktuella frågor. Som ovan anges påkallar den komplicerade karaktären i vissa frågor rörande skyldigheten att anmäla säkerhetsöverträdelser, inklusive huruvida det är lämpligt att införa undantag eller begränsningar, att dessa behandlas enhetligt, dvs. inom en enda lagstiftning som uteslutande tar upp denna fråga.

Samråd med Europeiska datatillsynsmannen och behovet av att bredda samrådet

40. Med tanke på hur mycket genomförandebestämmelserna kommer att påverka skyddet för människors personuppgifter är det viktigt att kommissionen, innan den beslutar om dessa bestämmelser, inleder ett vederbörligt samrådsförfarande. Därför välkomnar Europeiska datatillsynsmannen artikel 4.4 i förslaget, i vilken man uttryckligen fastställer att kommissionen ska samråda med Europeiska datatillsynsmannen innan den beslutar om genomförandebestämmelser. Dessa bestämmelser kommer inte endast att beröra utan även ha en inverkan på skyddet för enskildas personuppgifter och integritet. Det är därför viktigt att i enlighet med artikel 41 i förordning (EG) nr 45/2001 rådfråga Europeiska datatillsynsmannen.

41. Utöver samrådet med Europeiska datatillsynsmannen kan det vara lämpligt att införa en bestämmelse om att ett utkast till genomförandebestämmelser ska bli föremål för ett offentligt samråd i syfte att inhämta råd och uppmuntra till utbyte av bästa praxis på området. Detta kommer att ge inte endast näringslivet utan även andra berörda parter, inbegripet andra dataskyddsmyndigheter och artikel 29-gruppen, en passande kanal för att redovisa sina synpunkter. Behovet av ett offentligt samråd förstärks om man beaktar att det är kommittéförfarandet som gäller för antagande av lagstiftningen, med begränsat deltagande från Europaparlamentets sida.

42. Europeiska datatillsynsmannen noterar att man i artikel 4.4 i förslaget anger att kommissionen även ska samråda med myndigheten för marknaden för elektronisk kommunikation innan man beslutar om genomförandebestämmelser. Härvid värdesätter Europeiska datatillsynsmannen principen att man ska samråda med myndigheten för marknaden för elektronisk kommunikation såsom förvaltare av erfarenheten och kunskapen inom Europeiska byrån för nät- och informationssäkerhet om frågor rörande säkerhet för nät och information. Till dess att myndigheten för marknaden för elektronisk kommunikation har inrättats kan det vara lämpligt att som en tillfällig lösning i den föreslagna ändringen (artikel 4.4) ange samråd med Europeiska byrån för nät- och informationssäkerhet.

II.3 **Bestämmelsen om kakor, spionvara och liknande anordningar: ändring av artikel 5.3**

43. Artikel 5.3 i direktivet om integritet och elektronisk kommunikation tar upp frågan om teknik som möjliggör tillgång till information och lagring av information i användarens terminalutrustning via elektroniska kommunikationsnät. Ett exempel på tillämpningen av artikel 5.3 är användningen av kakor ([1]). Andra exempel omfattar användning av teknik som spionvara (dolda spionprogram) och trojanska hästar (program som är gömda i meddelanden eller i annan skenbart harmlös programvara). Målen för och syftena med denna teknik varierar enormt, varvid några är fullständigt ofarliga eller till och med användbara för användaren, medan andra syften helt tydligt är mycket farliga och hotfulla.

([1]) Kakor placeras av leverantörer av informationssamhällets tjänster (webbplatser) i användares terminalutrustning av olika skäl, bland annat för att känna igen en besökare när han/hon på nytt besöker en webbplats. I praktiken tilldelas användarens dator ett unikt nummer när en kaka sänds till en Internetanvändare från en webbplats, (dvs. den dator som fått kakor från webbplats A blir ”datorn med kaka 111”). Webbplatsen bevarar detta nummer som referens. Om den eller de användare av datorn som fått kaka 111 inte raderar kakfilen, kommer webbplatsen nästa gång som denne/dessa besöker samma webbplats att kunna identifiera datorn som innehavaren av kaka 111. Webbplatsen drar självfallet slutsatsen att denna dator har besökt webbplatsen tidigare. Den mekanism genom vilken en webbplats kan känna igen en dator som återbesökare är enkel. När den besökande datorn innehar kakor, exempelvis kaka 111, och besöker den webbplats som vid ett tidigare besök genererade samma kaka, kommer den att söka på användarens hårddisk efter kakans filnummer. Om användarens webbläsare finner en kakfil som matchar det referensnummer som webbplatsen bevarat, kommer den att informera webbplatsen om att datorn innehar en kaka 111.

44. I artikel 5.3 i direktivet om integritet och elektronisk kommunikation anges de villkor som ska tillämpas när man får tillgång till eller lagrar information i terminalutrustningen hos användare som bland annat använder ovan nämnda teknik. Enligt artikel 5.3 ska *i)* Internetanvändare ha tillgång till klar och fullständig information, bland annat om ändamålen med behandlingen, i enlighet med direktiv 95/46/EG, och *ii)* ha rätt att vägra sådan behandling, dvs. att avböja behandling av information som insamlats från hans/hennes terminalutrustning.

Nyttoeffekterna av den föreslagna ändringen

45. Genom den nu gällande artikel 5.3 i direktivet om integritet och elektronisk kommunikation begränsas tillämpningsområdet till situationer där tillgång till information och lagring av information i användarens terminalutrustning sker via *elektroniska kommunikationsnät*. Detta inbegriper vad som ovan beskrivs i fråga om användningen av kakor samt annan teknik som spionvara som sänds via elektroniska kommunikationsnät. Det är emellertid ingalunda klart om artikel 5.3 ska tillämpas i lägen där likartad teknik (kakor/spionvara och liknande) sprids via programvara som tillhandahålls inom externa lagringsmedier och laddas ner i användarens terminalutrustning. Med tanke på att hotet mot integriteten föreligger oberoende av kommunikationskanal är begränsningen till en kommunikationskanal i artikel 5.3 olycklig.

46. Europeiska datatillsynsmannen är sålunda nöjd med ändringen av artikel 5.3, vilken genom att man tar bort hänvisningen till ”elektroniska kommunikationsnät” i själva verket utvidgar tillämpningsområdet för artikel 5.3. Den ändrade versionen av artikel 5.3 omfattar situationer där tillgången till information och lagringen av information i användarens terminalutrustning sker via elektroniska kommunikationsnät men också via andra externa lagringsmedier för data som CD-skivor, CD-romskivor, USB-minnen m.m.

Teknisk lagring i syfte att underlätta överföringen

47. Den sista meningen i artikel 5.3 i direktivet om integritet och elektronisk kommunikation kvarstår oförändrad i den ändrade versionen av denna punkt. Enligt den sista meningen får kraven i artikel 5.3 första meningen ”inte förhindra någon teknisk lagring eller åtkomst som endast sker för att utföra eller underlätta överföringen av en kommunikation via ett elektroniskt kommunikationsnät eller som är absolut nödvändigt för att leverera en av informationssamhällets tjänster (…)”. Sålunda ska inte de tvingande bestämmelserna i artikel 5.3 första meningen (att information måste lämnas och att en möjlighet att vägra ska ges) tillämpas om användarens åtkomst till terminalutrustningen eller lagringen av information endast sker i syfte att *underlätta* en överföring eller om denna är absolut nödvändig för att tillhandahålla sådana informationssamhällets tjänster som användarna har begärt.

48. Det anges inte i direktivet när tillgången till eller lagringen av information endast har till syfte att underlätta en överföring eller att informera. En situation som avgjort omfattas av detta undantag är upprättandet av en Internetuppkoppling. Detta på grund av att det för att upprätta en Internetuppkoppling krävs att man erhållit en IP-adress ([1]). Slutanvändarens dator kommer att för Internetleverantören avslöja viss information om sig själv och Internetleverantören kommer att i gengäld ge honom en IP-adress. I detta fall kommer information som finns lagrad i slutanvändarens terminalutrustning att överföras till Internetleverantören i syfte att tillhandahålla användaren tillgång till Internet. I detta fall är Internetleverantören undantagen från både skyldigheten att tillkännage denna uppgiftsinsamling och från att ge rätt att vägra, om detta är nödvändigt för att tjänsten ska kunna levereras.

49. Om en användare, när han eller hon blivit ansluten till Internet, önskar besöka en viss webbplats, måste han/hon sända en begäran till den server som är värddator för webbplatsen. Denna kommer att svara om den vet vart den ska sända informationen, dvs. om den vet användarens IP-adress. Beroende på hur denna adress är lagrad, anmodar den åter den webbplats som användaren önskar besöka att få tillgång till information om Internetanvändarnas terminalutrustning. Helt uppenbart kommer även denna överföring att ligga inom räckvidden för undantaget. Det förefaller i dessa fall lämpligt att detta hålls utanför tillämpningsområdet för kraven i artikel 5.3.

([1]) En IP-adress (”Internet Protocol address”) är en unik adress som man inom viss elektronisk utrustning använder för att identifiera och kommunicera med varandra via ett datornät som använder standarden Internet Protocol (IP) – enklare uttryckt, en datoradress. Alla deltagande nätverksenheter – inbegripet routrar, växlar, datorer, servrar för infrastruktur (t.ex. NTP, DNS, DHCP, SNMP osv.), skrivare, faxar för Internet och vissa telefoner – kan ha sin egen adress som är unik inom det specifika nätet. Vissa IP-adresser är avsedda att vara unika inom hela det världsomspännande Internet medan andra endast behöver vara unika inom ett företag.

50. Europeiska datatillsynsmannen finner det lämpligt att göra undantag från behovet av att informera och ge möjlighet att vägra i situationer som de som det visats på ovan, när teknisk lagring eller åtkomst till en användares terminalutrustning är *nödvändig* för det blotta syftet att överföra ett meddelande via ett elektroniskt kommunikationsnät. Samma sak gäller när den tekniska lagringen eller åtkomsten är strikt nödvändiga för att tillhandahålla någon av informationssamhällets tjänster. Europeiska datatillsynsmannen finner dock inte att man behöver göra undantag från skyldigheten att informera och ge rätt att vägra i sådana lägen där den tekniska lagringen eller åtkomsten endast syftar till att *underlätta* överföringen av ett meddelande. Så får i enlighet med den sista meningen i denna artikel inte en registrerad person dra nytta av informationen och rätten att motsätta sig behandling av hans/hennes uppgifter om en kaka inhämtar uppgift om språkval eller geografiskt läge (t.ex. Belgien och Kina), eftersom detta slags kakor kan redovisas såsom syftande till att underlätta överföringen av ett meddelande. Europeiska datatillsynsmannen är medveten om att man i programvaror i praktiken ger registrerade personer möjlighet att vägra eller modulera lagringen av kakor. Detta har dock inte tillräckligt tydligt stöd i någon rättslig bestämmelse som formellt berättigar den registrerade personen att försvara sina rättigheter i den utsträckning som ovan anges.

51. För att undvika nämnda resultat föreslår Europeiska datatillsynsmannen att man ska företa en mindre ändring i den senare delen av artikel 5.3, vilken går ut på att man ska stryka ordet ”underlätta” i meningen: ”får inte förhindra någon teknisk lagring eller åtkomst som endast sker för att utföra eller underlätta överföringen av en kommunikation via ett elektroniskt kommunikationsnät eller som är absolut nödvändigt för att leverera en av informationssamhällets tjänster (…)”.

II.4 **Rättsliga åtgärder som vidtas av leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät samt av juridiska personer: tillägg av punkt 6 i artikel 13**

52. Genom den föreslagna artikel 13.6 föreskrivs civilrättsliga medel för enskilda eller juridiska personer med ett legitimt intresse, särskilt för leverantörer av elektroniska kommunikationstjänster som har ett affärsintresse av att bekämpa personer som bryter mot artikel 13 i direktivet om integritet och elektronisk kommunikation. Denna artikel tar upp sändandet av icke begärda meddelanden.

53. Den föreslagna ändringen kommer att göra det möjligt för exempelvis Internetleverantörer att bekämpa skräppostare för att dessa missbrukar deras nät, och att lagsöka organ som plagierar avsändaradresser eller bryter sig in i en server för att använda den som relästation för skräppost osv.

54. Direktivet om integritet och elektronisk kommunikation var inte tydligt vad gäller om det ger leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät rätt till åtgärder mot skräppostare och vid ytterst få tillfällen har leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät väckt talan inför domstol för brott mot artikel 13 såsom denna har omsatts i medlemsstatens lagstiftning ([1]). Genom erkännandet av rätt till rättsliga åtgärder för leverantörer av elektroniska kommunikationstjänster för att skydda sina affärsintressen bekräftar man i förslaget att direktivet om integritet och elektronisk kommunikation inte endast syftar till att skydda individuella abonnenter utan även leverantörerna av elektroniska kommunikationstjänster.

55. Europeiska datatillsynsmannen gläder sig över att man genom förslaget inför en möjlighet för leverantörer av elektroniska kommunikationstjänster som har ett affärsintresse av att väcka talan mot skräppostare. Utom under särskilda förhållanden har individuella abonnenter varken medel eller incitament att väcka denna typ av talan inför domstol. Däremot har andra Internetleverantörer än leverantörer av offentliga elektroniska kommunikationstjänster via allmänna nät den ekonomiska styrkan och de tekniska resurserna att undersöka skräppostkampanjer för att kartlägga gärningsmännen och det förefaller enbart vara på sin plats att de har rätt att vidta rättsliga åtgärder mot skräppostare.

56. Europeiska datatillsynsmannen värdesätter särskilt den föreslagna ändringen om den även möjliggör för konsumentorganisationer och fackföreningar som företräder intressena för konsumenter som erhållit skräppost att för deras räkning vidta rättsliga åtgärder inför domstol. Som ovan sagts är den skada som åsamkas en registrerad person som erhållit skräppost, om man ser det individuellt, vanligtvis i sig inte tillräcklig för att han/hon ska vidta rättsliga åtgärder inför domstol. I själva verket har Europeiska datatillsynsmannen redan i allmänna ordalag föreslagit den nämnda åtgärden i fråga

([1]) Ett fall där detta har inträffat är målet *Microsoft corporation* mot *Paul McDonald t/a Bizards UK* (2006 All Er (D) 153).

om integritetsintrång och dataskyddet i sitt yttrande om uppföljningen av arbetsprogrammet för ett bättre genomförande av dataskyddsdirektivet ([1]). Europeiska datatillsynsmannen anser att man i förslaget hade kunnat gå längre och föreslår kollektiv talan, varigenom man gör det möjligt för grupper av medborgare att gemensamt tillgripa rättsprövning i frågor som rör skyddet för personuppgifter. I fråga om skräppost, där ett stort antal personer erhåller skräppost, finns det en möjlighet för grupper av enskilda att gå samman och väcka kollektiv talan mot skräppostare.

57. Europeiska datatillsynsmannen beklagar i synnerhet att förslaget begränsar möjligheten för juridiska personer att vidta rättsliga åtgärder i relation till sådana förhållanden där det förekommer en överträdelse av artikel 13 i direktivet, dvs. situationer där det förekommer en överträdelse av bestämmelsen om icke begärd e-post. Enligt den föreslagna ändringen kommer juridiska personer inte att kunna vidta rättsliga åtgärder mot överträdelser av andra bestämmelser i direktivet om integritet och elektronisk kommunikation. Så gör inte den nu gällande bestämmelsen det möjligt för en juridisk person som en konsumentorganisation att vidta rättsliga åtgärder mot en Internetleverantör som avslöjat personuppgifter för miljontals kunder. Genomförandet av direktivet om integritet och elektronisk kommunikation som helhet, och inte endast av en viss artikel, skulle i hög grad förbättras om bestämmelsen i artikel 13.6 vidgades så att den gör det möjligt för juridiska personer att vidta rättsliga åtgärder mot överträdelser av alla bestämmelser i direktivet om integritet och elektronisk kommunikation.

58. För att lösa detta problem föreslår Europeiska datatillsynsmannen att man ska omvandla artikel 13.6 till en separat artikel (artikel 14). Dessutom bör formuleringen i artikel 13.6 ändras något på följande sätt: I stället för ”i enlighet med denna artikel” bör det stå ”i enlighet med detta direktiv”.

II.5 **Skärpta bestämmelser om genomförandet: tillägg av artikel 15a**

59. Direktivet om integritet och elektronisk kommunikation innehåller inga explicita bestämmelser om genomförandet. I stället hänvisar man till genomförandeavsnittet i dataskyddsdirektivet ([2]). Europeiska datatillsynsmannen välkomnar den nya artikel 15a i förslaget, som uttryckligen tar upp frågor rörande genomförandet av direktivet.

60. För det första noterar Europeiska datatillsynsmannen att en effektiv genomförandepolitik på området förutsätter, såsom det krävs i den föreslagna artikel 15a.3, att de nationella myndigheterna får utredningsbefogenheter för att kunna samla in nödvändiga uppgifter. Mycket ofta kommer beviset rörande en överträdelse av bestämmelser i direktivet om integritet och elektronisk kommunikation att vara av elektronisk art och eventuellt vara lagrat i olika datorer, anordningar eller nät. Det är i detta sammanhang viktigt att de brottsbekämpande organen får möjlighet att utverka husrannsakningsorder med befogenheter till inträde, husrannsakan och beslag.

61. För det andra välkomnar Europeiska datatillsynsmannen särskilt den föreslagna ändringen, dvs. artikel 15a.2, enligt vilken de nationella tillsynsmyndigheterna ska ha befogenhet att beordra förbudsförelägganden, dvs. att överträdelser upphör, och få de nödvändiga utredningsbefogenheterna och resurserna. De nationella tillsynsmyndigheterna, inbegripet nationella dataskyddsmyndigheter, bör ha befogenhet att besluta om förelägganden där lagbrytare förbjuds fortsätta en verksamhet som strider mot direktivet om integritet och elektronisk kommunikation. Förbudsförelägganden eller befogenhet att kräva att en överträdelse upphör är ett ändamålsenligt redskap vid ett pågående beteende som kränker individers rättigheter. Förbudsförelägganden kommer att bli mycket värdefulla när det gäller att hejda överträdelser av direktivet om integritet och elektronisk kommunikation som överträdelse av artikel 13 om icke begärd affärskommunikation, vilket till sin natur är ett pågående beteende.

62. För det tredje gör förslaget det möjligt för kommissionen att anta tekniska genomförandebestämmelser för att säkerställa ett effektivt gränsöverskridande samarbete i verkställandet av nationella lagar (föreslagen ändring av artikel 15a.4). I den hittillsvarande erfarenheten av samarbete ingår den överenskommelse som på kommissionens initiativ utformats om inrättande av ett gemensamt förfarande för att handlägga klagomål över gränserna mot skräppost.

([1]) Yttrande från Europeiska datatillsynsmannen om meddelandet från kommissionen till Europaparlamentet och rådet om uppföljningen av arbetsprogrammet för ett bättre genomförande av dataskyddsdirektivet (EUT C 255, 27.10.2007, s. 1).

([2]) 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.

63. Europeiska datatillsynsmannen anser att det obestridligen kommer att stödja den gränsöverskridande verkställigheten om lagstiftningen ger stöd för att tillsynsmyndigheter ska få bistå sina motsvarigheter i andra länder. Det är därför lämpligt att man i direktivet ger kommissionen möjlighet att skapa förutsättningar för säkerställandet av gränsöverskridande samarbete, vilket inbegriper förfarandena för informationsutbyte.

III SLUTSATSER OCH REKOMMENDATIONER

64. Europeiska datatillsynsmannen välkomnar till fullo förslaget. De föreslagna ändringarna stärker skyddet för enskildas integritet och personuppgifter inom sektorn för elektronisk kommunikation, och detta sker med ett ringa ingrepp och utan att man lägger oberättigade och onödiga bördor på organisationerna. På ett mer konkret plan anser Europeiska datatillsynsmannen att de föreslagna ändringarna i flertalet fall inte bör ändras i den mån som de vederbörligen uppfyller det mål som man eftersträvar. I punkt 69 nedan förtecknas de ändringar om vilka Europeiska datatillsynsmannen hoppas att de kvarstår oförändrade.

65. Trots den övergripande positiva bedömningen av förslaget anser Europeiska datatillsynsmannen att vissa av ändringarna i det bör förbättras för att sörja för att de på ett effektivare sätt ger ett ordentligt skydd för personuppgifterna och enskildas integritet. Detta gäller framför allt i fråga om bestämmelserna om anmälan av säkerhetsöverträdelser och om de bestämmelser som behandlar rättsliga åtgärder som vidtas av leverantörer av elektroniska kommunikationstjänster för överträdelse av bestämmelser om skräppost. Dessutom beklagar Europeiska datatillsynsmannen att man inte i förslaget tar sig an vissa frågor som inte behandlas på tillfredsställande sätt i det nu gällande direktivet om integritet och elektronisk kommunikation, och därigenom missar tillfället inom denna översyn att lösa de kvarstående problemen.

66. För att lösa båda problemen, dvs. frågor som inte på tillfredsställande sätt tas upp i förslaget och frågor som över huvud taget inte behandlas, läggs det i detta yttrande fram ett vissa förslag till formuleringar. I punkterna 67 och 68 sammanfattas problemen och det föreslås här konkreta formuleringar. Europeiska datatillsynsmannen uppmanar de lagstiftande organen att beakta dessa när förslaget passerar genom lagstiftningsförfarandet.

67. De ändringar i förslaget, i vilka Europeiska datatillsynsmannen på det bestämdaste vill förorda en ändring, utgörs av följande:

i) **Anmälan av säkerhetsöverträdelser**: Som den är formulerad gäller den föreslagna ändringen, genom vilken *artikel 4.4* läggs till, leverantörer av elektroniska kommunikationstjänster via allmänna nät (Internetleverantörer, nätoperatörer), vilka åläggs att anmäla säkerhetsöverträdelser till de nationella tillsynsmyndigheterna och till sina kunder. Europeiska datatillsynsmannen stöder till fullo denna skyldighet men anser dock att den även bör gälla leverantörer av informationssamhällets tjänster, vilka ofta behandlar känsliga personuppgifter. Sålunda bör Internetbanker och försäkringsbolag med verksamhet via Internet, leverantörer av hälso- och sjukvård via Internet och alla andra Internetföretag också vara tvungna att uppfylla denna skyldighet.

Europeiska datatillsynsmannen föreslår därför att man i artikel 4.3 även omnämner leverantörerna av informationssamhällets tjänster enligt följande: ”Vid en säkerhetsöverträdelse (…) ska leverantören av allmänt tillgängliga elektroniska kommunikationstjänster och leverantören av informationssamhällets tjänster (…) meddela den berörda abonnenten och den berörda nationella tillsynsmyndigheten denna överträdelse”.

ii) **Rättsliga åtgärder som vidtas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster via allmänna nät**: Som den är formulerad ger den föreslagna ändringen, genom vilken *artikel 13.6* läggs till, civilrättsliga medel för enskilda eller juridiska personer, framför allt för leverantörer av elektroniska kommunikationstjänster, att bekämpa överträdelser av artikel 13 i direktivet om integritet och elektronisk kommunikation som behandlar skräppost. Europeiska datatillsynsmannen är tillfreds med denna bestämmelse. Europeiska datatillsynsmannen ser dock inte något motiv för att denna nya kapacitet ska begränsas till överträdelse av artikel 13. Europeiska datatillsynsmannen föreslår att man ska göra det möjligt för juridiska personer att vidta rättsliga åtgärder mot överträdelse av alla bestämmelser i direktivet om integritet och elektronisk kommunikation.

För att uppnå detta föreslår Europeiska datatillsynsmannen att man ska omvandla artikel 13.6 till en separat artikel (artikel 14). Dessutom bör formuleringen i artikel 13.6 ändras något på följande sätt: I stället för ”i enlighet med denna artikel” bör det stå ”i enlighet med detta direktiv”.

68. Tillämpningsområdet för direktivet om integritet och elektronisk kommunikation som för närvarande är begränsat till tillhandahållare av allmänna elektroniska kommunikationsnät är en av de besvärligaste frågor på vilken förslaget inte ger någon lösning. Europeiska datatillsynsmannen anser att direktivet bör ändras, så att dess tillämpningsområde vidgas till att inbegripa leverantörer av elektroniska kommunikationstjänster, även i blandade (privata/offentliga) och privata nät.

69. De ändringar som Europeiska datatillsynsmannen på det bestämdaste vill förorda att de kvarstår oförändrade utgörs av följande:

i) **RFID**: Den föreslagna ändringen i *artikel 3*, enligt vilken elektroniska kommunikationsnät ska inbegripa ”allmänna kommunikationsnät som stöder datainsamling och identifikationsutrustning”, är fullt tillräcklig. Denna bestämmelse är mycket positiv eftersom man genom den förtydligar att antal RFID-tillämpningar måste följa direktivet om integritet och elektronisk kommunikation, varigenom man undanröjer viss rättslig osäkerhet på denna punkt.

ii) **Kakor/spionvara**: Den föreslagna ändringen i *artikel 5.3* bör välkomnas eftersom den medför att skyldigheten att informera och ge rätt att motsätta sig att kakor/spionvara lagras i den egna terminalutrustningen även kommer att gälla när sådan utrustning placeras via externa lagringsmedier för data som CD-skivor, CD-romskivor och USB-minnen. Europeiska datatillsynsmannen föreslår dock att en mindre ändring ska företas i den senare delen av artikel 5.3, vilken går ut på att man i meningen ska stryka ordet ”underlätta”.

iii) **Valet av kommittéförfarande tillsammans med samråd med Europeiska datatillsynsmannen och villkor för/begränsningar av skyldigheten att göra anmälan**: Med den föreslagna ändringen, genom vilken man lägger till artikel 4.4 om anmälan av säkerhetsöverträdelser, överlåts beslut i komplicerade frågor rörande omständigheterna/formen/förfarandena för systemet för anmälan av säkerhetsöverträdelser till ett kommittéförfarande, efter det att man begärt råd från Europeiska datatillsynsmannen. Europeiska datatillsynsmannen stöder kraftfullt denna enhetliga modell. Lagstiftningen om anmälan av säkerhetsöverträdelser är ett ämnesområde som behöver tas upp efter en omsorgsfull debatt och analys.

Kopplad till denna fråga är begäran från vissa intressenter om utformande av undantag från skyldigheten att anmäla säkerhetsöverträdelse i artikel 4.4. Europeiska datatillsynsmannen motsätter sig kraftfullt denna uppläggning och förordar i stället att det övergripande ämnet för anmälan, hur anmälan ska göras, under vilka omständigheter som anmälan kan förkortas eller på något sätt begränsas ska analyseras i ett helhetsperspektiv, efter vederbörlig debatt.

iv) **Genomförande**: Den föreslagna ändringen, genom vilken *artikel 15a* läggs till, innehåller många behjälpliga inslag som bör bibehållas och kommer att bidra till att säkerställa faktisk efterlevnad, vilket inbegriper förstärkandet av de nationella tillsynsmyndigheternas undersökande befogenheter (artikel 15a.3) och införandet av en befogenhet för de nationella tillsynsmyndigheterna att kräva att överträdelser upphör.

Utfärdat i Bryssel den 10 april 2008.

Peter HUSTINX

Europeiska datatillsynsmannen