I

(Beslutninger og resolutioner, henstillinger og udtalelser)

UDTALELSER

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om forslag til Europa-Parlamentets og Rådets direktiv om ændring af bl.a. direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation)

(2008/C 181/01)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

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

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

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

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

som henviser til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger, særlig artikel 41 ([3]),

som henviser til Kommissionens anmodning om udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001, der blev modtaget den 16. november 2007,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. **INDLEDNING**

1. Den 13. november 2007 vedtog Kommissionen et forslag til et direktiv om ændring af bl.a. direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (i det følgende benævnt »forslaget« eller »ændringsforslaget«). Den nuværende version af direktiv 2002/58/EF benævnes sædvanligvis e-databeskyttelsesdirektivet, også i denne udtalelse.

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

2. Forslaget går ud på at styrke beskyttelsen af den enkeltes privatliv og personoplysninger i den elektroniske kommunikationssektor. Dette gøres ikke ved fuldstændigt at omarbejde det gældende e-databeskyttelsesdirektiv, men derimod ved at foreslå ad hoc-ændringer heraf, som hovedsagelig har til formål at styrke de sikkerhedsrelaterede bestemmelser og forbedre håndhævelsesmekanismerne.

3. Forslaget er led i en større reform af de fem EU-telekommunikationsdirektiver (»telekommunikationspakken«). Ud over forslagene til revision af telekommunikationspakken ([1]) har Kommissionen samtidig også vedtaget et forslag til en forordning om oprettelse af Den Europæiske Myndighed for Markedet for Elektronisk Kommunikation ([2]).

4. Bemærkningerne i denne udtalelse begrænses til ændringsforslagene til e-databeskyttelsesdirektivet, medmindre sådanne ændringsforslag er baseret på begreber eller bestemmelser i forslagene til revision af telekommunikationspakken. Herudover er der et antal bemærkninger i denne udtalelse, der har relation til bestemmelser i e-databeskyttelsesdirektivet, der ikke ændres ved forslaget.

5. Denne udtalelse behandler følgende emner: *i)* anvendelsesområdet for e-databeskyttelsesdirektivet, navnlig de berørte tjenester (ændringsforslag til artikel 3, stk. 1); *ii)* anmeldelse af brud på sikkerheden (ændringsforslag om indsættelse af artikel 4, stk. 3, og artikel 4, stk. 4); *iii)* bestemmelserne om »cookies«, spionsoftware og lignende udstyr (ændringsforslag til artikel 5, stk. 3); *iv)* retslige skridt, der tages af udbydere af elektroniske kommunikationstjenester og andre juridiske personer (ændringsforslag om indsættelse af artikel 13, stk. 6), og *v)* stramning af håndhævelsesbestemmelserne (ændringsforslag om indsættelse af en ny artikel 15a).

Høring af den tilsynsførende og bredere offentlig høring

6. Kommissionen sendte forslaget til den tilsynsførende den 16. november 2007. Den tilsynsførende opfatter denne meddelelse som en anmodning om at rådgive fællesskabsinstitutionerne og -organerne som omhandlet i artikel 28, stk. 2, i forordning (EF) nr. 45/2001 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Fællesskabets institutioner og organer og om fri udveksling af sådanne oplysninger (i det følgende benævnt »forordning (EF) nr. 45/2001«).

7. Forud for vedtagelsen af forslaget hørte Kommissionen uformelt den tilsynsførende om udkastet til forslag, som den tilsynsførende hilste velkommen, da det gav ham lejlighed til at fremkomme med en række forslag til udkastet til forslag, før det blev vedtaget af Kommissionen. Den tilsynsførende er glad for at se, at nogle af hans forslag afspejles i forslaget.

8. Forud for vedtagelsen af forslaget blev der gennemført en bred høring af offentligheden, en praksis, som den tilsynsførende sætter pris på. I juni 2006 igangsatte Kommissionen således en offentlig høring om meddelelsen om revisionen af telekommunikationspakken, hvor Kommissionen beskrev sit syn på situationen og fremsatte en række ændringsforslag ([3]). Artikel 29-Gruppen vedrørende Beskyttelse af Personoplysninger, som den tilsynsførende er medlem af, benyttede denne lejlighed til at fremkomme med sine synspunkter om ændringsforslagene i en udtalelse, der blev vedtaget den 26. september 2006 ([4]).

([1]) Ændringsforslagene til telekommunikationsdirektiverne er fremsat i følgende forslag: *i)* Forslag til Europa-Parlamentets og Rådets direktiv om ændring af direktiv 2002/21/EF om fælles rammebestemmelser for elektroniske kommunikationsnet og tjenester, direktiv 2002/19/EF om adgang til og samtrafik mellem elektroniske kommunikationsnet og tilhørende faciliteter og direktiv 2002/20/EF om tilladelser til elektroniske kommunikationsnet og -tjenester, KOM(2007) 697 endelig af 13.11.2007, *ii)* Forslag til Europa-Parlamentets og Rådets direktiv om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om forbrugerbeskyttelsessamarbejde, KOM(2007) 698 endelig af 13.11.2007.

([2]) Forslag til Europa-Parlamentets og Rådets forordning om oprettelse af Den Europæiske Myndighed for Markedet for Elektronisk Kommunikation, KOM(2007) 699 endelig af 13.11.2007.

([3]) Meddelelse af 29. juni 2006 om EU's regelsæt for elektroniske kommunikationsnet og -tjenester (SEK(2006) 816). Meddelelsen blev suppleret af et arbejdsdokument fra Kommissionens tjenestegrene (KOM(2006) 334 endelig).

([4]) Udtalelse 8/2006 af 26. september 2006 om revision af rammebestemmelserne for elektronisk kommunikation og elektroniske tjenester, med fokus på e-databeskyttelsesdirektivet.

Den tilsynsførendes overordnede synspunkter

9. Generelt ser den tilsynsførende positivt på forslaget. Den tilsynsførende støtter fuldt ud Kommissionens hensigt om at vedtage et forslag, der styrker beskyttelsen af den enkeltes privatliv og personoplysning i den elektroniske kommunikationssektor. Den tilsynsførende ser med særlig tilfredshed på vedtagelsen af et system til obligatorisk anmeldelse af brud på sikkerheden (ændring til artikel 4 i e-databeskyttelsesdirektivet ved tilføjelse af stk. 3 og 4). Når der forekommer brud på datasikkerheden indebærer anmeldelse klare fordele, det styrker organisationernes ansvarlighed, det er en faktor, der tilskynder virksomhederne til at gennemføre stringente sikkerhedsforanstaltninger, og det giver mulighed for at finde frem til de mest pålidelige teknologier med henblik på at beskytte oplysninger. Herudover giver det de berørte enkeltpersoner lejlighed til at tage skridt til at beskytte sig selv mod identitetstyveri eller anden misbrug af deres personlige oplysninger.

10. Den tilsynsførende hilser andre ændringer i forslaget velkommen, som f.eks. muligheden af, at juridiske personer med en legitim interesse kan anlægge søgsmål mod dem, der overtræder bestemmelser i e-databeskyttelsesdirektivet (ændring til artikel 13 ved tilføjelse af stk. 6). Det er ligeledes positivt, at de nationale tilsynsmyndigheder får styrket deres undersøgelsesbeføjelser, da det vil sætte dem i stand til at vurdere, om alle former for databehandling foretages i overensstemmelse med loven og til at finde frem til lovovertræderne (tilføjelse af artikel 15a, stk. 3). At kunne standse ulovlig behandling af personoplysninger og krænkelser af privatlivets fred så hurtigt som muligt er en nødvendig foranstaltning for at beskytte personers rettigheder og frihedsrettigheder. I denne forbindelse ses der med stor tilfredshed på den foreslåede artikel 15a, stk. 2, hvori de nationale tilsynsmyndigheder får beføjelse til at kræve ophør af overtrædelserne, da det vil sætte dem i stand til at bringe groft ulovlig databehandling til øjeblikkeligt ophør.

11. Tilgangen i forslaget og de fleste af ændringsforslagene er i overensstemmelse med synspunkterne på den fremtidige databeskyttelsespolitik, som er blevet fremsat i tidligere udtalelser fra den tilsynsførende, som f.eks. udtalelsen om gennemførelsen af databeskyttelsesdirektivet ([1]). Tilgangen er bl.a. baseret på den overbevisning, at selv om det ikke er nødvendigt med nye databeskyttelsesprincipper, er der behov for mere specifikke regler til at tackle de databeskyttelsesspørgsmål, der rejses på grund af nye teknologier som internettet, RFID, osv. samt redskaber, der bidrager til at styrke og effektivisere databeskyttelseslovgivningen, såsom at give juridiske personer mulighed for at indlede søgsmål for krænkelse af databeskyttelsen og at give registeransvarlige pligt til at anmelde brud på datasikkerheden.

12. På trods af forslagets generelt positive tilgang beklager den tilsynsførende, at forslaget ikke er så ambitiøst, som det kunne have været. Siden 2003 har anvendelsen af bestemmelserne i e-databeskyttelsesdirektivet samt en omhyggelig analyse af emnet vist, at en del af bestemmelserne deri langt fra er klare, og at de forårsager retlig usikkerhed og problemer med overholdelsen. For eksempel er dette tilfældet med hensyn til spørgsmålet om, i hvilket omfang halvoffentlige udbydere af elektroniske kommunikationstjenester er omfattet af e-databeskyttelsesdirektivet. Man kunne have håbet, at Kommissionen vil have benyttet sig af revisionen af telekommunikationspakken, og navnlig af e-databeskyttelsesdirektivet, til at løse nogle af de udestående problemer. Endvidere indeholder forslagets tilgang til nye spørgsmål, såsom indførelse af et obligatorisk system til anmeldelse af brud på datasikkerheden, kun en delvis løsning, der ikke omfatter organisationer med pligt til at anmelde brud på sikkerheden, enheder, der behandler meget følsomme typer af data, såsom online-banker eller udbydere af online-sundhedstjenester. Den tilsynsførende beklager denne tilgang.

13. Den tilsynsførende håber, at efterhånden som forslaget kommer gennem lovgivningsprocessen, vil lovgiveren tage hensyn til bemærkningerne og forslagene i denne udtalelse med henblik på løsning af de spørgsmål, som Kommissionens forslag forsømmer at behandle.

([1]) Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse af 25. juli 2007 om meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om opfølgning på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet, EUT C 255 af 27.10.2007, s. 1.

II. ANALYSE AF FORSLAGET

II.1. Anvendelsesområde for e-databeskyttelsesdirektivet, navnlig de berørte tjenester

14. Et af nøglespørgsmålene i det nuværende e-databeskyttelsesdirektiv er dets anvendelsesområde. Forslaget indeholder en række positive elementer, der medvirker til at definere og præcisere direktivets anvendelsesområde, navnlig hvilke tjenester, der er berørt af direktivet, og som behandles nedenfor i afsnit i). Desværre løser ændringsforslagene ikke alle de eksisterende problemer. Som det fremgår af afsnit ii), søger ændringerne desværre ikke at udvide direktivets anvendelsesområde til at omfatte elektroniske kommunikationstjenester i private netværk.

15. Artikel 3 i e-databeskyttelsesdirektivet beskriver de tjenester, der er berørt af direktivet, med andre ord, de tjenester, som forpligtelserne i direktivet gælder for: »Dette direktiv finder anvendelse på behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet«.

16. Således er de tjenester, der er omfattet af e-databeskyttelsesdirektivet, udbydere af offentlige elektroniske kommunikationstjenester i offentlige net. Definitionen af udbydere af kommunikationstjenester i offentlige net findes i artikel 2, litra c), i rammedirektivet ([1]). Offentlige kommunikationsnet er defineret i artikel 2, litra d), i rammedirektivet ([2]). Eksempler på aktiviteter, der udøves af udbydere af offentlige kommunikationstjenester i offentlige net omfatter ydelse af adgang til internettet, transmission af oplysninger via elektroniske net, mobiltelefonforbindelser og telefonforbindelser, osv.

i) *Ændringsforslag til artikel 3 i e-databeskyttelsesdirektivet: de berørte tjenester skal omfatte offentlige kommunikationsnet med dataindsamlings- og identifikationsudstyr*

17. Forslaget ændrer artikel 3 i e-databeskyttelsesdirektivet ved at præcisere, at offentlige elektroniske kommunikationsnet omfatter »offentlige kommunikationsnet med dataindsamlings- og -identifikationsudstyr«. Det fremgår af betragtning 28, at udvikling af applikationer, der indebærer indsamling af oplysninger, herunder personoplysninger, under anvendelse af radiofrekvenser såsom RFID, er underlagt e-databeskyttelsesdirektivet, når de forbindes eller anvender offentlige kommunikationsnet eller -tjenester.

18. Den tilsynsførende finder, at denne bestemmelse er positiv, da den præciserer, at en række RFID-applikationer falder ind under e-databeskyttelsesdirektivets anvendelsesområde og således fjerner en vis usikkerhed på dette punkt og definitivt fjerner misforståelser og fejlfortolkninger af loven.

19. I henhold til den nuværende artikel 3 i e-databeskyttelsesdirektivet er visse RFID-applikationer faktisk allerede dækket af direktivet. Dette gælder af flere akkumulerende grunde. For det første fordi RFID-applikationer hører ind under definitionen på elektroniske kommunikationstjenester. For det andet fordi de udbydes via et elektronisk kommunikationsnet, for så vidt applikationerne understøttes af et transmissionssystem, der overfører signaler trådløst. Og endelig kan nettet være offentligt eller

([1]) Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (2002), EFT L 108 af 24.4.2002, s. 33. Rammedirektivet afgrænser, hvad der skal forstås ved elektroniske kommunikationstjenester, nemlig: i) En »elektronisk kommunikationstjeneste« er en tjeneste, som normalt ydes mod betaling, og som består i overføring af signaler via net, herunder telekommunikationstjenester og transmissionstjenester på net. ii) Tjenester, der består i tilrådighedstillelse af indhold fremført via elektroniske kommunikationsnet og -tjenester, er ikke omfattet af definitionen af elektroniske kommunikationstjenester. iii) Udbud af tjenester: etablering, drift, styring eller tilrådighedstillelse af et net. iv) Elektroniske kommunikationstjenester omfatter ikke informationssamfundstjenester, der er defineret i e-handelsdirektivet som en tjeneste/tjenester, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager.

([2]) »Offentligt kommunikationsnet«: et elektronisk kommunikationsnet, som udelukkende eller overvejende bruges til udbud af offentligt tilgængelige elektroniske kommunikationstjenester.

privat. Hvis det er offentligt, vil RFID-applikationer blive betragtet som »berørte tjenester« og således falde ind under anvendelsesområdet for e-databeskyttelsesdirektivet. Imidlertid vil den foreslåede ændring eliminere enhver resterende tvivl herom og således give mere juridisk sikkerhed.

20. Som nævnt i en tidligere udtalelse fra den tilsynsførende om RFID ([1]), udelukker denne bestemmelse naturligvis ikke, at der kan være behov for at vedtage yderligere retsakter for så vidt angår RFID. Sådanne foranstaltninger bør dog vedtages i en anden kontekst, ikke som del af dette forslag.

ii) *Behov for at medtage elektroniske kommunikationstjenester i private eller halvprivate net*

21. Den tilsynsførende hilser de ovenfor beskrevne præciseringer velkommen, men beklager dog, at forslaget ikke har behandlet spørgsmålet om den stadig mere uklare skelnen mellem private og offentlige net. Endvidere beklager den tilsynsførende, at definitionen på tjenester ifølge e-databeskyttelsesdirektivet ikke er blevet udvidet til at omfatte private net. Som situationen er nu, gælder artikel 3, stk. 1, i e-databeskyttelsesdirektivet kun for elektroniske kommunikationstjenester i offentlige net.

22. Den tilsynsførende noterer at der er en tendens til, at tjenester i stadig højere grad bliver en blanding af private og offentlige tjenester. Tænk for eksempel på universiteter, der tillader tusinder af studerende at bruge internet og e-mail. Sådanne halvoffentlige (eller halvprivate) nets mulighed for at indvirke på privatlivets fred for den enkelte er åbenbar og denne type tjenester bør derfor underlægges samme regelsæt, som der gælder for rent offentlige net. Endvidere har private net såsom net tilhørende arbejdsgivere, der giver de ansatte internetadgang, hoteller eller lejlighedsejere, der stiller telefon og e-mail til rådighed for gæsterne, samt internetcaféer indvirkning på databeskyttelsen og privatlivets fred for brugerne, hvilket lægger op til, at de også bør være omfattet af anvendelsesområdet for e-databeskyttelsesdirektivet.

23. Faktisk har retspraksis i visse medlemsstater allerede behandlet elektroniske kommunikationstjenester, der udbydes i private net, efter de samme forpligtelser, som der gælder for tjenester, der udbydes af offentlige net ([2]). Endvidere har databeskyttelsesmyndighederne i henhold til tysk lov fundet, at det at give privat e-mailadgang i en virksomhed kan bevirke, at virksomheden anses som udbyder af offentlige telekommunikationstjenester og derfor falder ind under bestemmelserne i e-databeskyttelsesdirektivet.

24. Kort sagt berettiger den stadig større betydning af blandede (private/offentlige) og private net i dagligdagen, med en tilsvarende stadig større risiko for den personlige datasikkerhed og privatlivets fred, til at det er nødvendigt at anvende samme regelsæt på sådanne tjenester som det, der gælder for offentlige elektroniske kommunikationstjenester. Med henblik herpå er det den tilsynsførendes opfattelse, at direktivet bør ændres, så anvendelsesområdet udvides til at omfatte denne type private tjenester; et synspunkt, der deles af Artikel 29-Gruppen ([3]).

II.2. **Underretning om brud på sikkerheden: Ændring af artikel 4**

25. Artikel 4 i e-databeskyttelsesdirektivet ændres ved, at der indsættes to nye stykker (stk. 3 og 4), der indeholder en forpligtelse til at underrette om brud på sikkerheden. I henhold til artikel 4, stk. 3, er udbyderen af offentligt tilgængelige kommunikationstjenester på den ene side forpligtet til uden unødig forsinkelse at underrette de nationale tilsynsmyndigheder om alle brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles i forbindelse med udbuddet af offentligt tilgængelige kommunikationstjenester (samlet benævnt »datalækage«); på den anden side er udbyderen også forpligtet til at underrette deres kunder.

([1]) Udtalelse af 20. december 2007 om meddelelsen fra Kommissionen til Europa-Parlamentet, Rådet, det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om radiofrekvensbaseret identifikation (RFID) i Europa: elementer til en politisk ramme, KOM(2007) 96.

([2]) For eksempel hedder det i dom afsagt den 4. februar 2005 af appeldomstolen i Paris i sagen *BNP Paris mod World Press Online*, at der ikke er forskel mellem udbydere af internettjenester, der tilbyder internetadgang på kommercielt grundlag, og arbejdsgivere, der giver deres personale internetadgang.

([3]) Udtalelse 8/2006 af 26. september 2006 om revision af rammebestemmelserne for elektronisk kommunikation og elektroniske tjenester, med fokus på e-databeskyttelsesdirektivet.

Fordele ved denne forpligtelse

26. Den tilsynsførende er tilfreds med disse bestemmelser (artikel 4, stk. 3, og artikel 4, stk. 4), der indfører en pligt til underretning om sikkerhedsbrud. Underretning om sikkerhedsbrud har positive virkninger set ud fra et perspektiv om beskyttelse af personoplysninger og privatlivets fred, der allerede har været afprøvet i USA, hvor de enkelte stater allerede for flere år siden indførte lovgivning om underretning om sikkerhedsbrud.

27. For det første gør lovgivning om underretning af sikkerhedsbrud udbyderen af offentligt tilgængelige kommunikationstjenester mere ansvarlig for de oplysninger, der er lækket. Inden for rammerne af databeskyttelse eller politikken om privatlivets fred betyder ansvarliggørelse, at hver eneste organisation er ansvarlig for de oplysninger, der er i dens varetægt og under dens kontrol. Forpligtelsen til underretning er ensbetydende med, at det endnu en gang fastslås, dels at de lækkede oplysninger henhørte under udbyderens kontrol, dels at det er denne organisations ansvar at træffe de nødvendige foranstaltninger med hensyn til sådanne oplysninger.

28. For det andet har eksistensen af underretning om sikkerhedsbrud vist sig at være en faktor, der fremmer investeringer i sikkerhed i organisationer, der behandler personoplysninger. Alene den omstændighed, at organisationer offentligt skal underrette om sikkerhedsbrud, får dem til at gennemføre strengere sikkerhedsnormer, som beskytter personoplysninger og forebygger sikkerhedsbrud. Endvidere vil underretning om sikkerhedsbrud bidrage til at kortlægge og foretage pålidelige statistiske analyser af de mest effektive sikkerhedsløsninger og -mekanismer. Der har i længere tid manglet hårde data om informationssikkerhedssvigt og om de teknologier, der er mest hensigtsmæssige til at beskytte oplysninger. Problemet vil sandsynligvis blive løst med forpligtelsen til underretning om sikkerhedsbrud, som tilfældet var med de amerikanske love om underretning om sikkerhedsbrud, fordi en sådan underretning vil give oplysninger om, hvilke teknologier der er mest udsatte for sikkerhedsbrud ([1]).

29. Endelig gør underretning om sikkerhedsbrud den enkelte bevidst om den risiko, man løber, når ens personoplysninger lækkes, og hjælper den pågældende med at træffe de nødvendige foranstaltninger for at reducere sådanne risici. Hvis der f.eks. lækkes bankoplysninger, kan den person, der underrettes, beslutte at ændre sine adgangsoplysninger til bankkontoen for at hindre andre i at overtage disse oplysninger og bruge dem til et ulovligt formål (sædvanligvis benævnt »identitetstyveri«). Denne forpligtelse gør det mindre sandsynligt, at personer bliver ofre for identitetstyveri og kan også hjælpe ofrene med at træffe de foranstaltninger, der er nødvendige for at løse problemerne.

Mangler ved den foreslåede ændring

30. Selv om den tilsynsførende er tilfreds med den ordning for underretning om sikkerhedsbrud, der indføres med artikel 4, stk. 3, og artikel 4, stk. 4, ville han have foretrukket, at artiklerne kunne anvendes mere bredt, så også udbydere af informationssamfundstjenester blev omfattet. Dette ville betyde, at onlinebanker, onlinevirksomheder, onlineudbydere af sundhedstjenester, etc. også ville være omfattet af loven ([2]).

31. De grunde, der berettiger til, at udbydere af offentligt tilgængelige elektroniske kommunikationstjenester pålægges at underrette om sikkerhedsbrud, gælder også for andre organisationer, der også behandler enorme mængder personoplysninger, hvis afsløring kan være meget skadelig for de registrerede. Dette omfatter onlinebanker, »data brokers« (firmaer, der sælger personoplysninger), og andre onlineudbydere såsom dem, der behandler følsomme oplysninger (bl.a. oplysninger om sundhed, politiske synspunkter, etc.). Lækage af oplysninger fra onlinebanker og -virksomheder kan omfatte ikke blot bankkontonumre, men også kreditkortoplysninger, kan medføre identitetstyveri, og det er da afgørende, at de pågældende personer bliver varskoet, så de kan træffe de nødvendige foranstaltninger. I tilfælde af onlinesundhedsoplysninger lider de berørte personer måske ikke økonomisk skade, men kan lide ikke-økonomisk skade, hvis følsomme oplysninger lækkes.

([1]) Se rapporten »Security Economics and the Internal Market« (de økonomiske følger af sikkerhed og det indre marked) udarbejdet af Prof. Ross Anderson, Rainer Böhme, Richard Clayton og Tyler Moore på bestilling af ENISA. Rapporten er tilgængelig på http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Udbydere af informationssamfundstjenester defineres i e-databeskyttelsesdirektivet som enhver tjeneste/tjenester, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager.

32. Ved en udvidelse af forpligtelsens anvendelsesområde vil ovennævnte fordele, som indførelsen af denne forpligtelse forventes at give, endvidere ikke være begrænset til blot den ene sektor af udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, men vil blive udvidet til at omfatte informationssamfundstjenester generelt. Hvis informationssamfundstjenester såsom onlinebanker pålægges forpligtelser til underretning om sikkerhedsbrud, vil disse aktører ikke blot blive gjort mere ansvarlige, men det vil også motivere dem til at styrke deres sikkerhedsforanstaltninger, og fremtidige potentielle sikkerhedsbrud vil således kunne undgås.

33. Der er andre fortilfælde, hvor e-databeskyttelsesdirektivet allerede gælder for andre enheder end udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, såsom artikel 5 om kommunikationshemmelighed og artikel 13 om spam. Dette bekræfter, at lovgiveren tidligere meget klogt besluttede at udvide anvendelsesområdet for visse bestemmelser i e-databeskyttelsesdirektivet, fordi man mente, det var hensigtsmæssigt og nødvendigt. Den tilsynsførende håber, at lovgiveren ikke vil tøve med nu at følge en lignende fornuftig og fleksibel fremgangsmåde og vil udvide anvendelsesområdet for artikel 4 til også at omfatte udbydere af informationssamfundstjenester. Det vil med henblik herpå være tilstrækkeligt at indsætte følgende ordlyd vedrørende udbyderne af informationssamfundstjenester i artikel 4, stk. 3: »Sker der brud på sikkerheden, der fører til hændelig eller … skal udbyderen af offentligt tilgængelige kommunikationstjenester og udbyderen af informationssamfundstjenester (…) underrette den berørte abonnent og den nationale tilsynsmyndighed om bruddet«.

34. Den tilsynsførende ser denne forpligtelse og anvendelsen af den på udbydere af offentligt tilgængelige elektroniske kommunikationstjenester såvel som på udbydere af informationssamfundstjenester som første etape i en udvikling, der til sidst vil kunne anvendes på alle registeransvarlige generelt.

Specifik juridisk ramme for sikkerhedsbrud, der skal behandles ved komitologi

35. Forslaget behandler ikke en række af de spørgsmål, der vedrører forpligtelsen til at underrette om sikkerhedsbrud. Eksempler på spørgsmål, der skal behandles, er omstændighederne omkring underretningen, og det format og de procedurer, der skal anvendes. I stedet giver forslagets artikel 4, stk. 4, mulighed for, at sådanne beslutninger vedtages af et »komitologiudvalg« ([1]), nemlig Kommunikationsudvalget, der er nedsat ved artikel 22 i rammedirektivet, ifølge Rådets afgørelse af 28. juni 1999. Sådanne foranstaltninger skal vedtages i overensstemmelse med artikel 5 i Rådets afgørelse af 28. juni 1999, der fastsætter regler for forskriftsproceduren for så vidt angår »generelle foranstaltninger, der har til formål at gennemføre væsentlige bestemmelser i basisretsakter«.

36. Den tilsynsførende modsætter sig ikke, at man vælger at overlade alle disse spørgsmål til gennemførelseslovgivningen. Vedtagelse af lovgivning gennem komitologi vil sandsynligvis gøre lovgivningsproceduren kortere. Komitologi vil også bidrage til at sikre harmonisering, som man bør have som endemål.

37. Under hensyn til de mange spørgsmål, der skal behandles i gennemførelsesbestemmelserne, og relevansen af dem som fremhævet nedenfor vil det være hensigtsmæssigt at tackle dem samlet i én retsakt i stedet for hver for sig, hvorved nogle af spørgsmålene ville blive behandlet i e-databeskyttelsesdirektivet og andre ville blive overladt til gennemførelseslovgivningen. Kommissionens fremgangsmåde, der består i at overlade disse beslutninger til gennemførelseslovgivningen, der skal vedtages efter høring af den tilsynsførende og forhåbentlig også andre interessenter (jf. næste punkt), vil derfor være den bedste.

Spørgsmål, der skal behandles gennem gennemførelsesforanstaltninger

38. Gennemførelsesforanstaltningerne bliver mere relevante, hvis man forholdsvis detaljeret kan forudsige, hvilke spørgsmål der skal behandles ved gennemførelsesforanstaltninger. Gennemførelsesforanstaltninger kan faktisk være bestemmende for, hvilke standarder underretningerne skal foretages efter. De kan f.eks. specificere, hvad der er et sikkerhedsbrud, betingelserne for, hvornår der skal foretages underretninger til enkeltpersoner og til myndigheder, tidspunktet for underretningen og selve underretningen.

([1]) Lovgivningsprocedurer i EF, der involverer udvalg bestående af repræsentanter for medlemsstaternes regeringer på tjenestemandsniveau.

39. Den tilsynsførende mener ikke, at e-databeskyttelsesdirektivet, og især artikel 4, bør indeholde en undtagelse fra forpligtelsen til underretning. I den forbindelse er den tilsynsførende tilfreds med Kommissionens fremgangsmåde, der er fastlagt i artikel 4, og som opstiller en forpligtelse til at underrette og ikke indeholder en undtagelse herfra, men giver mulighed for, at dette og andre spørgsmål kan behandles i gennemførelseslovgivningen. Selv om den tilsynsførende ved, at der er argumenter, der taler for at indføre visse undtagelser fra forpligtelsen, går den tilsynsførende ind for, at dette og andre spørgsmål behandles omhyggeligt i gennemførelseslovgivningen efter en grundig og samlet drøftelse af alle de spørgsmål, der er tale om. Som nævnt ovenfor taler de komplekse spørgsmål vedrørende forpligtelsen til underretning om sikkerhedsbrud, herunder om undtagelser eller begrænsninger er hensigtsmæssige, for, at dette behandles samlet, dvs. i én retsakt, der udelukkende omhandler dette spørgsmål.

Høring af den tilsynsførende og behovet for at udvide høringen

40. I betragtning af hvor meget gennemførelsesforanstaltningerne vil påvirke beskyttelsen af det enkelte menneskes personoplysninger, er det vigtigt, at Kommissionen foretager en passende høring, inden sådanne foranstaltninger vedtages. Den tilsynsførende er derfor tilfreds med forslagets artikel 4, stk. 4, hvor det udtrykkeligt hedder, at Kommissionen hører den europæiske tilsynsførende for databeskyttelse, inden gennemførelsesforanstaltningerne vedtages. Sådanne foranstaltninger vil ikke blot berøre, men have en stor virkning for beskyttelsen af personoplysninger og det enkelte menneskes privatliv. Det er derfor vigtigt at søge rådgivning fra den tilsynsførende, jf. artikel 41 i forordning (EF) nr. 45/2001.

41. Foruden høringen af den tilsynsførende kan det være hensigtsmæssigt at indsætte en bestemmelse om, at udkast til gennemførelsesforanstaltninger skal være genstand for offentlig høring med henblik på rådgivning og tilskyndelse til at dele erfaringer vedrørende bedste praksis på disse områder. Dette vil være en passende kanal, hvor ikke blot erhvervslivet men også andre interessenter, herunder andre databeskyttelsesmyndigheder og Artikel 29-Gruppen, kan fremsætte deres synspunkter. Behovet for offentlig høring bliver større, hvis man tager hensyn til, at der ved vedtagelsen af lovgivning anvendes udvalgsprocedure med begrænset deltagelse fra Europa-Parlamentets side.

42. Den tilsynsførende bemærker, at der i forslagets artikel 4, stk. 4, står, at Kommissionen også vil høre Den Europæiske Myndighed for Markedet for Elektronisk Kommunikation, inden gennemførelsesbestemmelserne vedtages. I den forbindelse værdsætter den tilsynsførende princippet om høring af Den Europæiske Myndighed for Markedet for Elektronisk Kommunikation som depositar for ENISA's erfaringer og viden om net- og informationssikkerhedsspørgsmål. Indtil Den Europæiske Myndighed for Markedet for Elektronisk Kommunikation er oprettet, kan det være hensigtsmæssigt i den foreslåede ændring (artikel 4, stk. 4) at nævne høring af ENISA som en overgangsløsning.

II.3. **Bestemmelser om cookies, spyware og lignende anordninger: ændring af artikel 5, stk. 3:**

43. Artikel 5, stk. 3, i e-databeskyttelsesdirektivet omhandler spørgsmålet om teknologier, der giver mulighed for adgang til og lagring af oplysninger i brugernes terminaludstyr via elektroniske kommunikationsnet. Et eksempel på anvendelsen af artikel 5, stk. 3, er brugen af cookies ([1]). Andre eksempler er anvendelsen af teknologier såsom spyware (skjulte spionprogrammer) og trojanske heste (programmer, der er skjult i meddelelser eller i anden tilsyneladende uskyldig software). Formålet med sådanne teknologier varierer meget, nogle er fuldstændig uskadelige eller endda nyttige for brugeren, hvorimod andre klart er meget skadelige og udgør en trussel.

([1]) Cookies anbringes af udbydere af informationssamfundstjenester (websteder) i brugernes terminaludstyr til forskellige formål, bl.a. til at genkende en besøgende, når han/hun gensøger et websted. I praksis sker der det, når et websted sender en cookie til en internetbruger, at brugerens computer tildeles et unikt nummer (f.eks. bliver den computer, der modtager cookies fra websted A, »indehaver af cookie 111«). Webstedet beholder dette nummer som en reference. Hvis brugeren/brugerne af den computer, der modtog cookie 111, ikke sletter cookie-filen, vil webstedet kunne identificere computeren som indehaver af cookie 111, næste gang den pågældende besøger samme websted. Webstedet udleder naturligvis, at denne computer har besøgt stedet tidligere. Den mekanisme, som gør, at webstedet genkender en computer som en genbesøger, er enkel. Når den besøgende computer indeholder cookies som cookie 111 og besøger det websted, som ved et tidligere besøg genererede denne cookie, søger den efter cookie-filnummeret på brugerens harddisk. Hvis brugerens browser finder en cookie-fil, der svarer til referencenummeret hos webstedet, informerer den webstedet om, at computeren indeholder en cookie 111.

44. I artikel 5, stk. 3, i e-databeskyttelsesdirektivet omhandles de betingelser, der finder anvendelse, når der opnås adgang til eller lagres oplysninger i brugernes terminaludstyr bl.a. ved hjælp af ovennævnte teknologier. I henhold til artikel 5,stk. 3, nr. *i)* skal internetbrugere have klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen i overensstemmelse med direktiv 95/46/EF, og i henhold til nr. *ii)* skal internetbrugere have ret til at nægte en sådan behandling, dvs. vælge at afvise behandling af oplysninger, der er hentet fra hans/hendes terminaludstyr.

Fordele ved den foreslåede ændring

45. Den eksisterende artikel 5, stk. 3, i e-databeskyttelsesdirektivet begrænser anvendelsesområdet til situationer, hvor adgang til og lagring af oplysninger i brugernes terminaludstyr foregår via *elektroniske kommunikationsnet*. Dette omfatter den situation, der beskrives ovenfor, med brug af cookies og andre teknologier såsom spyware, der leveres via elektroniske kommunikationsnet. Det er dog langt fra klart, om artikel 5, stk. 3, finder anvendelse i situationer, hvor lignende teknologier, (cookies/spyware og lignende) distribueres ved hjælp af software, der leveres på eksterne lagringsmedier og downloades til brugernes terminaludstyr. Da truslen mod privatlivets fred findes uanset kommunikationskanalen, er det uheldigt, hvis artikel 5, stk. 3, begrænses til kun én kommunikationskanal.

46. Den tilsynsførende er derfor tilfreds med ændringen til artikel 5, stk. 3, som ved at fjerne henvisningen til »elektroniske kommunikationsnet« reelt udvider anvendelsesområdet for artikel 5, stk. 3. Faktisk omfatter den ændrede udgave af artikel 5, stk. 3, både situationer, hvor adgang til informationer og lagring af informationer i brugerens terminaludstyr sker via elektroniske kommunikationsnet, men også via andre eksterne datalagringsmedier såsom CD'er, CD-rom'er, USB-nøgler, osv.

Teknisk lagring med henblik på at lette overføring

47. Sidste punktum i artikel 5, stk. 3, i e-databeskyttelsesdirektivet ændres ikke i den ændrede udgave. I henhold til sidste punktum, er kravene i første punktum i artikel 5, stk. 3, »ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre eller lette overføring af kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at levere en informationssamfundstjeneste (…)«. Derfor vil de obligatoriske regler i første punktum i artikel 5, stk. 3, (pligten til at give oplysninger og give mulighed for at nægte) ikke gælde, når adgang til brugerens terminaludstyr eller lagring af oplysninger alene sker med det formål at *lette* overføring eller, når det er absolut påkrævet for at levere informationssamfundstjenester, som brugeren ønsker.

48. Direktivet beskriver ikke, hvornår adgang til eller lagring af oplysninger alene har til formål at lette overføring eller give oplysninger. En situation, som klart vil være omfattet af denne undtagelse, er oprettelse af en internetforbindelse. Dette skyldes, at det for at oprette en internetforbindelse, er nødvendigt at få en IP-adresse ([1]). Slutbrugerens computer vil blive bedt om at afgive visse oplysninger om sig selv til udbyderen af internetadgangen, og til gengæld vil udbyderen af internetadgangen tildele den en IP-adresse. I dette tilfælde vil oplysninger lagret i slutbrugerens terminaludstyr blive overført til udbyderen af internetadgangen med det formål at give brugeren adgang til internettet. I så fald undtages udbyderen af internetadgangen fra både pligten til at anmelde denne indsamling af oplysninger og til at give ret til at nægte, for så vidt det er nødvendigt for at levere tjenesten.

49. Når brugeren er forbundet med internettet må denne, hvis han eller hun ønsker at se en given webside, sende en anmodning til den server, der er vært for websiden. Sidstnævnte vil svare, hvis den ved, hvor den skal sende oplysningerne hen, dvs. hvis den kender brugerens IP-adresse. På grund af den måde, som adressen er lagret på, kræver det igen, at den webside, som brugeren ønsker at besøge, får adgang til oplysninger på internetbrugerens terminaludstyr. Denne transaktion vil helt klart også falde ind under undtagelsen. Faktisk synes det i disse tilfælde at være hensigtsmæssigt at befinde sig uden for anvendelsesområdet for kravene i artikel 5, stk. 3.

([1]) En IP-adresse (internetprotokoladresse) er en unik adresse, som visse former for elektronisk udstyr anvender for at identificere hinanden og kommunikere indbyrdes med hinanden på et edb-net under anvendelse af internetprotokolstandarden (IP) — mere enkelt sagt, en computeradresse. Alt involveret netudstyr — herunder routere, kontakter, computere, infrastrukturservere (f.eks. NTP, DNS, DHCP, SNMP, osv.), printere, internetfaxmaskiner og visse telefoner — kan have sin egen adresse, der er unik inden for rammerne af det specifikke net. Nogle IP-adresser er udformet med henblik på at være unikke på det globale internet, medens andre kun behøver at være unikke inden for rammerne af en virksomhed.

50. Den tilsynsførende finder det hensigtsmæssigt at se bort fra behovet for at informere og give mulighed for at nægte i situationer som nævnt ovenfor, hvor teknisk lagring eller adgang til en brugers terminaludstyr er *nødvendig* alene med det formål at overføre kommunikation via et elektronisk kommunikationsnet. Det samme gør sig gældende, når teknisk lagring eller adgang er absolut påkrævet for at levere en informationssamfundstjeneste. Den tilsynsførende ser imidlertid ikke noget behov for at se bort fra forpligtelsen til at give oplysninger og give ret til at nægte i de situationer, hvor teknisk lagring eller adgang sker alene med det formål at *lette* overføring af kommunikation. For eksempel bliver den registrerede i medfør af denne artikels sidste punktum muligvis ikke informeret eller får ikke ret til at modsætte sig behandling af sine oplysninger, hvis en cookie indsamler oplysninger om hans sprogpræferencer eller lokalisering (f.eks. Belgien eller Kina), da denne type cookies kan præsenteres, som om deres formål er at lette overføring af kommunikation. Den tilsynsførende er opmærksom på, at de registrerede på softwareniveau får mulighed for i praksis at nægte eller ændre lagring af cookies. Dette er der imidlertid ikke tilstrækkelig tydelig juridisk opbakning til, da der ikke er nogen juridiske bestemmelser, der formelt giver den registrerede ret til at forsvare sine rettigheder i situationer som beskrevet ovenfor.

51. For at undgå dette foreslår den tilsynsførende en mindre ændring af sidste del af artikel 5, stk. 3, der består i at lade udtrykket »eller lette overføring af« udgå af dette punktum: »er ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre eller lette overføring af kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at levere en informationssamfundstjeneste (…)«.

II.4. **Søgsmål anlagt af udbydere af offentlige elektroniske kommunikationsnet og -tjenester samt af juridiske personer Tilføjelse af stk. 6 til artikel 13**

52. Forslaget til artikel 13, stk. 6, giver søgsmålsret til en fysisk eller juridisk person med en legitim interesse, navnlig udbydere af elektroniske kommunikationstjenester, der måtte have en forretningsinteresse i at bekæmpe overtrædelser af artikel 13 i e-databeskyttelsesdirektivet. Denne artikel omhandler udsendelse af uønskede reklamehenvendelser.

53. Den foreslåede ændring giver f.eks. udbydere af internetadgang lov til at tage sig af spammere, der misbruger deres net, sagsøge enheder, der forfalsker afsenderadresser eller hacker servere for at bruge dem til formidling af spam, osv.

54. I e-databeskyttelsesdirektivet var det ikke klart, om udbydere har ret til at anlægge sag mod spammere, og udbyderne har kun ved meget få lejligheder lagt sag an for overtrædelse af artikel 13 som gennemført i medlemsstaternes lovgivning ([1]). Ved at anerkende, at udbydere af elektroniske kommunikationstjenester har ret til at lægge sag an for at beskytte deres forretningsinteresser, bekræfter forslaget, at e-databeskyttelsesdirektivet har til formål ikke blot at beskytte individuelle abonnenter men også udbydere af elektroniske kommunikationstjenester.

55. Den tilsynsførende er tilfreds med, at forslaget giver udbydere af elektroniske kommunikationstjenester med en forretningsinteresse mulighed for at anlægge sag mod spammere. Bortset fra under særlige omstændigheder har individuelle abonnenter hverken penge eller incitament til at indlede en sag af denne art. I modsætning hertil har udbydere af internetadgang og andre udbydere økonomisk styrke og teknologisk kapacitet til at efterforske spamkampagner, identificere ophavsmændene, og det synes kun rimeligt, at de har ret til at tage retslige skridt mod spammere.

56. Den tilsynsførende sætter særlig stor pris på ændringsforslaget, fordi det også vil give forbrugerorganisationer og handelsforeninger, der repræsenterer forbrugere, der har fået tilsendt spam, mulighed for at indbringe sagen for domstolene på deres vegne. Som beskrevet ovenfor er den skade, som en registreret, der har fået tilsendt spam, udsættes for individuelt set normalt ikke i sig selv tilstrækkelig til, at han/hun kan indbringe sagen for domstolene. Rent faktisk foreslog den tilsynsførende allerede denne foranstaltning for så vidt angår krænkelser af privatlivets fred og databeskyttelsesovertrædelser

([1]) Et eksempel på dette er sagen Microsoft corporation vs. Paul McDonald t/a Bizards UK (2006 All ER (D) 153).

generelt i sin udtalelse om opfølgningen på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet ([1]). Ifølge den tilsynsførendes mening kunne forslaget have gået endnu videre og foreslået kollektive søgsmål, der sætter grupper af borgere i stand til i fællesskab at lægge sag an i spørgsmål vedrørende beskyttelse af personoplysninger. Når det drejer sig om spam, hvor et stort antal mennesker modtager spam, er der mulighed for, at disse enkeltpersoner kan gå sammen i grupper og anlægge kollektive søgsmål mod spammere.

57. Den tilsynsførende beklager især, at forslaget begrænser juridiske personers mulighed for at tage retslige skridt i situationer, hvor der er tale om en overtrædelse af direktivets artikel 13, dvs. i tilfælde, hvor der er tale om en overtrædelse af bestemmelsen om uønsket kommunikation via e-mail. Faktisk har juridiske personer ved den foreslåede ændring ikke mulighed for at tage retslige skridt over for overtrædelser af andre bestemmelser i e-databeskyttelsesdirektivet. For eksempel giver den nugældende bestemmelse ikke en juridisk person — eksempelvis en forbrugerorganisation — mulighed for at anlægge sag mod en udbyder af internetadgang, der har offentliggjort personoplysninger på millioner af kunder. Håndhævelsen af e-databeskyttelsesdirektivet som helhed og ikke blot af en enkelt artikel ville blive væsentligt forbedret, hvis bestemmelsen i artikel 13, stk. 6, blev gjort generel, så juridiske personer kunne lægge sag an for overtrædelse af enhver bestemmelse i e-databeskyttelsesdirektivet.

58. For at løse dette problem foreslår den tilsynsførende, at stk. 6 i artikel 13 ændres til en særskilt artikel (artikel 14). Herudover bør artikel 13, stk. 6, ændres en smule og affattes således: »i medfør af denne artikel« ændres til »i medfør af dette direktiv«.

II.5. **Styrkelse af retshåndhævelsesbestemmelserne: tilføjelse af artikel 15a**

59. E-databeskyttelsesdirektivet indeholder ikke nogen eksplicitte håndhævelsesbestemmelser. I stedet henviser det til afsnittet om håndhævelse i e-databeskyttelsesdirektivet ([2]). Den tilsynsførende ser med tilfredshed på den nye artikel 15a i forslaget, der eksplicit omhandler håndhævelsesspørgsmål i forbindelse med dette direktiv.

60. For det første bemærker den tilsynsførende, at en effektiv håndhævelsespolitik på dette område forudsætter, som det også kræves i forslagets artikel 15a, stk. 3, at de nationale myndigheder har efterforskningsbeføjelser med henblik på at skaffe sig de nødvendige oplysninger. Meget ofte vil beviserne på, at der er sket en overtrædelse af bestemmelserne i e-databeskyttelsesdirektivet være af elektronisk art og bliver eventuelt lagret på forskellige computere og medier eller net. I den forbindelse er det vigtigt, at de retshåndhævende myndigheder får mulighed for at få en dommerkendelse, så de har beføjelse til at få adgang, søge og beslaglægge.

61. For det andet ser den tilsynsførende især med tilfredshed på den foreslåede ændring i artikel 15a, stk. 2, i henhold til hvilken de nationale tilsynsmyndigheder skal have beføjelse til at nedlægge påstand om et forbud, dvs. at bringe overtrædelser til ophør, og have de nødvendige ressourcer og beføjelser til efterforskning. De nationale tilsynsmyndigheder, herunder de nationale databeskyttelsesmyndigheder, bør have beføjelse til at nedlægge påstand om et forbud, så lovovertrædere forhindres i at fortsætte en adfærd, der er en overtrædelse af e-databeskyttelsesdirektivet. Forbud eller beføjelser til få bragt en overtrædelse til ophør er et nyttigt redskab, hvis der er tale om en vedvarende adfærd, der krænker enkeltpersoners rettigheder. Forbud vil være meget nyttige til at bringe overtrædelser af e-databeskyttelsesdirektivet til ophør, f.eks. overtrædelse af artikel 13 om uønskede reklamehenvendelser, der i kraft af selve deres art er en vedvarende adfærd.

62. For det tredje giver forslaget Kommissionen mulighed for at træffe tekniske gennemførelsesforanstaltninger med henblik på at sikre et effektivt samarbejde over grænserne for så vidt angår håndhævelse af de nationale love (foreslået ændring, artikel 15a, stk. 4). De hidtidige samarbejdserfaringer omfatter en aftale på Kommissionens initiativ om oprettelse af en fælles procedure til behandling af klager over spam på tværs af grænserne.

([1]) Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om opfølgning på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet (EUT C 255 af 27.10.2007, s. 1).

([2]) Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

63. Den tilsynsførende mener, at det, hvis lovgivningen støtter lovgiverne i at bistå lovgiverne i andre lande, uden tvivl vil gavne håndhævelsen på tværs af grænserne. Det er derfor fornuftigt, at forslaget giver Kommissionen mulighed for at skabe de rette betingelser for at sikre samarbejdet på tværs af grænserne, herunder procedurerne for udveksling af oplysninger.

III. **KONKLUSIONER OG ANBEFALINGER**

64. Den tilsynsførende hilser forslaget meget velkommen. De foreslåede ændringer styrker beskyttelsen af privatlivets fred og personoplysninger i den elektroniske kommunikationssektor, og dette gøres med let hånd uden at pålægge organisationerne uberettigede og unødvendige byrder. Mere specifikt finder den tilsynsførende, at størstedelen af de foreslåede ændringer ikke bør ændres, for så vidt som de opfylder det forfulgte mål korrekt. Under punkt 69 nedenfor findes en liste over de ændringer, som den tilsynsførende håber, forbliver uændrede.

65. Uanset sin generelt set positive holdning til forslaget finder den tilsynsførende, at visse af ændringerne bør forbedres, så det sikres, at de yder en effektiv beskyttelse af personoplysninger og privatlivets fred. Dette gør sig især gældende for bestemmelserne om underretning om sikkerhedsbrud og de bestemmelser, der omhandler søgsmål anlagt af udbydere af elektroniske kommunikationstjenester for overtrædelse af bestemmelserne om spam. Den tilsynsførende beklager i øvrigt, at der er spørgsmål, forslaget ikke kommer ind på, og som ikke er ordentligt dækket i det nugældende e-databeskyttelsesdirektiv, og det er derfor ikke i forbindelse med denne revision lykkedes at løse de udestående spørgsmål.

66. Med henblik på at løse begge problemer, dvs. både spørgsmål, der ikke er løst tilstrækkelig godt i forslaget, og spørgsmål, som man slet ikke kommer ind på, er der i denne udtalelse stillet nogle formuleringsforslag. I punkt 67 og 68 sammenfattes spørgsmålene, og der foreslås en konkret affattelse. Den tilsynsførende opfordrer lovgiveren til at tage dem til efterretning, efterhånden som forslaget går igennem lovgivningsprocessen.

67. De ændringer i forslaget, hvor den tilsynsførende meget gerne ser en ændring, er følgende:

i) **Underretning om sikkerhedsbrud**: Som nævnt finder den foreslåede ændring med en tilføjelse af *artikel 4, stk. 4,* anvendelse på udbydere af offentlige elektroniske kommunikationstjenester i offentlige net (internetudbydere og netoperatører), som er forpligtet til at underrette de nationale tilsynsmyndigheder og kunderne om sikkerhedsbrud. Den tilsynsførende bakker fuldt ud op om denne forpligtelse. Den tilsynsførende mener imidlertid, at forpligtelsen også bør omfatte udbydere af informationssamfundstjenester, der ofte behandler følsomme personoplysninger. Således vil onlinebanker og -forsikringsselskaber, onlineudbydere af sundhedstjenester og andre onlinevirksomheder også skulle opfylde denne forpligtelse.

Det vil med henblik herpå være tilstrækkeligt at indsætte følgende tekst vedrørende udbyderne af informationssamfundstjenester i artikel 4, stk. 3: »Sker der brud på sikkerheden, (…) skal udbyderen af offentligt tilgængelige kommunikationstjenester og udbyderen af informationssamfundstjenester (…) underrette den berørte abonnent og den nationale tilsynsmyndighed om bruddet«.

ii) **Søgsmål anlagt af udbydere af offentlige elektroniske kommunikationstjenester i offentlige net**: Som nævnt giver den foreslåede ændring om tilføjelse af *stk. 6 til artikel 13* mulighed for, at en fysisk eller juridisk person, navnlig udbydere af elektroniske kommunikationstjenester, kan anlægge sag for at bekæmpe overtrædelse af artikel 13 i e-databeskyttelsesdirektivet, der omhandler spam. Den tilsynsførende er tilfreds med denne bestemmelse. Den tilsynsførende kan imidlertid ikke se fornuften i, at denne nye mulighed skal begrænses til kun at omfatte overtrædelse af artikel 13. Den tilsynsførende foreslår, at juridiske personer får mulighed for at tage retslige skridt over for overtrædelse af alle bestemmelser i e-databeskyttelsesdirektivet.

For at opnå dette foreslår den tilsynsførende, at stk. 6 i artikel 13 ændres til en særskilt artikel (artikel 14). Herudover bør artikel 13, stk. 6, ændres en smule og affattes således: »i medfør af denne artikel« ændres til »i medfør af dette direktiv«.

68. E-databeskyttelsesdirektivets anvendelsesområde, der i øjeblikket er begrænset til at omfatte udbydere af offentlige elektroniske kommunikationsnet, er et af de mest bekymrende spørgsmål, som forslaget ikke kommer ind på. Den tilsynsførende finder, at direktivet bør ændres, så anvendelsen udvides til også at omfatte udbydere af elektroniske kommunikationstjenester i blandede (private/offentlige) og private net.

69. De ændringer, som den tilsynsførende meget gerne ser forblive uændrede, er følgende:

i) **RFID**: Den foreslåede ændring af *artikel 3*, hvorved elektroniske kommunikationsnet omfatter »offentlige kommunikationsnet med dataindsamlings- og identifikationsudstyr« er fuldt ud tilfredsstillende. Det er meget positivt, at denne bestemmelse findes, da den tydeliggør, at en række RFID-anvendelser skal opfylde bestemmelserne i e-databeskyttelsesdirektivet og således fjerner en vis juridisk usikkerhed på dette punkt.

ii) **Cookies/spyware**: Den foreslåede ændring af *artikel 5, stk. 3*, hilses velkommen, fordi den betyder, at forpligtelsen til at orientere og retten til at modsætte sig, at cookies/spyware lagres i ens terminaludstyr, også finder anvendelse, når sådanne anordninger anbringes via eksterne datalagringsmedier, såsom CD-rom'er og USB-nøgler. Den tilsynsførende foreslår dog en mindre ændring af sidste del af artikel 5, stk. 3, der består i at lade udtrykket »eller lette overføring af« udgå af dette punktum.

iii) **Valg af udvalgsproceduren i samråd med den tilsynsførende og betingelser for/begrænsning af underretningspligten**: Den foreslåede ændring med tilføjelse af artikel 4, stk. 4, vedrørende underretning om sikkerhedsbrud lader det være op til et udvalg efter høring af den tilsynsførende at træffe beslutningerne i komplekse problemstillinger vedrørende forhold, format og procedurer for ordningen for underretning om sikkerhedsbrud. Den tilsynsførende støtter fuldt ud denne ensartede tilgang. Lovgivning om underretning om sikkerhedsbrud er et særligt område, som der skal fastsættes regler for efter nærmere drøftelse og undersøgelse.

I tilknytning til dette spørgsmål melder der sig visse parters anmodning om indførelse af undtagelser fra pligten til at underrette om sikkerhedsbrud i artikel 4, stk. 4. Den tilsynsførende er meget imod denne tilgang. Han går derimod ind for, at hele spørgsmålet om underretning, hvordan den skal foregå, under hvilke omstændigheder underretningen kan forkortes eller begrænses, skal indgå i en helhedsbetragtning efter en grundig debat.

iv) **Håndhævelse**: Den foreslåede ændring om tilføjelse af *artikel 15a* indeholder mange nyttige elementer, der skal bevares, og som vil være med til at sikre effektiv overholdelse, herunder styrkelse af de nationale tilsynsmyndigheders efterforskningsbeføjelser (artikel 15a, stk. 3) og indførelse af beføjelse til de nationale tilsynsmyndigheder til at få bragt overtrædelser til ophør.

Udfærdiget i Bruxelles, den 10. april 2008.

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse