EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 22.01.2004
KOM(2004) 28 slutlig

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN OCH REGIONKOMMITTÉN

om icke begärd kommersiell kommunikation eller så kallad skräppost

INNEHÅLLSFÖRTECKNING

MEDDELANDE FRÅN KOMMISSIONEN
TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN OCH REGIONKOMMITTÉN

om icke begärd kommersiell kommunikation eller så kallad skräppost

(Text av betydelse för EES)

SAMMANFATTNING

Icke begärd kommersiell kommunikation via e-post, även kallad skräppost, har antagit oroväckande proportioner. Mer än 50 % av den globala e-posttrafiken beräknas bestå av skräppost. Ännu mer oroväckande är hastigheten med vilken denna andel ökar: 2001 uppgick siffran till ”bara” 7 %.

Skräppost är ett problem av flera skäl: integritetsskydd, vilseledning av konsumenter, skydd av minderåriga och den mänskliga värdigheten, extrakostnader för företag, produktivitetsförlust. På ett mer allmänt plan undergräver skräpposten konsumenternas förtroende och hindrar därmed utvecklingen av e-handeln, e-tjänster och informationssamhället.

EU förutsåg denna fara och införde därför i juli 2002, genom direktiv 2002/58/EG om integritet och elektronisk kommunikation, principen om samtyckesbaserad marknadsföring (opt-in) för e-post (inklusive SMS- respektive MMS-meddelanden på mobiltelefon) samt kompletterande skyddsmekanismer för konsumenter. Sista dagen för direktivets genomförande var den 31 oktober 2003. Kommissionen har inlett överträdelseförfaranden mot en rad medlemsstater som inte har anmält sina genomförandeåtgärder.

Att införa ny lagstiftning är ett första och viktigt steg, men det löser bara en del av problemet. I detta meddelande beskrivs de åtgärder som krävs för att komplettera EU-reglerna och omsätta skräppostförbudet i praktiken.

Det finns dock inga patentlösningar på skräppostproblemet. De åtgärder som beskrivs i detta meddelande är framför allt inriktade på medlemsstaternas och myndigheternas verkställande av gällande regler, på tekniska lösningar och självreglering inom näringslivet och på ökad konsumentmedvetenhet. Särskild uppmärksamhet riktas också mot den internationella dimensionen, eftersom mycket skräppost kommer från länder utanför EU.

Åtgärderna bygger visserligen på det samförstånd som uppnåddes under 2003 och som bekräftades vid en offentlig workshop i oktober 2003, men det är också viktigt att enas om hur åtgärderna skall genomföras. Skräppostens ökning kan bara begränsas om alla drar sitt strå till stacken, dvs. både medlemsstater och myndigheter, liksom företag, konsumenter och användare av Internet och elektronisk kommunikation.

En del åtgärder är förbundna med kännbara kostnader, men det är priset man måste betala om e-post och e-tjänster även i framtiden skall fungera som effektiva kommunikationsverktyg.

Genomförandet av de åtgärder som beskrivs i detta meddelande kommer att bidra till en avsevärd minskning av skräpposten, till gagn för informationssamhället och EU:s medborgare och ekonomier.

Bakgrund och syfte

Icke begärd kommersiell kommunikation via e-post[1], dvs. skräppost, uppfattas nuförtiden allmänt som ett av de största problemen på Internet. Skräpposten har antagit oroväckande proportioner. Det finns risk att e-post- och SMS-användare helt enkelt slutar använda mobila tjänster och e-post, som är en av de mest omtyckta Internettillämpningarna, eller att de begränsar användningen på ett sätt som de annars inte hade gjort. Skräpposten måste uppmärksammas mer, eftersom Internet och annan elektronisk kommunikation (t.ex. bredband, trådlös kommunikation, mobilkommunikation) på ett avgörande sätt förväntas bidra till produktivitetstillväxten i de moderna ekonomierna.

Det råder visserligen samförstånd om att man måste ingripa innan den ökande skräpposten tillintetgör e-postens och andra e-tjänsters fördelar för företag och medborgare, men det är inte lika klart hur skräpposten bäst skall bekämpas. Framför allt finns det inga patentlösningar på problemet. En effektiv bekämpning av skräpposten är bara möjlig om alla drar sitt strå till stacken, dvs. både medlemsstater och behöriga myndigheter, liksom företag, konsumenter och användare av Internet och elektronisk kommunikation.

I detta meddelande beskrivs olika rättsliga, tekniska och medvetenhetsökande åtgärder på grundval av direktiv 2002/58/EG, där det fastställs ett samtyckesbaserat opt-in-system för kommersiell kommunikation som medlemsstaterna skulle ha infört senast den 31 oktober 2003[2].

Åtgärderna är framför allt inriktade på ett effektivt genomförande och verkställande av direktivet i medlemsstaterna, tekniska lösningar, självregling inom näringslivet, ökad konsumentmedvetenhet och internationellt samarbete. Den internationella dimensionen är särskilt viktig, eftersom mycket skräppost verkar komma från länder utanför EU, framför allt Nordamerika[3].

Åtgärderna bygger på det samförstånd som uppnåddes under 2003 och som bekräftades vid en offentlig workshop i oktober 2003[4].

---

1 Meddelandet gäller inte icke begärd kommunikation utanför Internet, t.ex. icke begärd post.

2 Se särskilt artikel 13 i direktiv 2002/58/EG om integritet och elektronisk kommunikation (se avsnitt 2 nedan).

3 Att Förenta staterna, och i något mindre utsträckning även Kanada, är de främsta skräppostkällorna verkar exempelvis bekräftas av de initiativ till en e-postlåda för skräppostklagomål som 2002 togs av franska ”Commission Nationale Informatique et Libertés” (CNIL) och belgiska ”Commission de la Protection de la Vie Privée” (CPVP). CPVP:s resultat återfinns på http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf. CNIL:s rapport återfinns på http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf. Se även UNCTAD, *E-Commerce and Development Report 2003*, New York och Genève, 2003, s. 27.

4 Inför denna workshop delades det ut ett diskussionsunderlag om skräppost. Diskussionsunderlaget byggde på tidigare diskussioner inom kommunikationskommittén (COCOM) och med artikel 29-

Samförstånd på området är viktigt inte minst för att det främst är upp till de berörda parterna att med kommissionens stöd genomföra åtgärderna till gagn för informationssamhället, näringslivet och användarna.

Dokumentets struktur

I dokumentet delas skräppostproblemet upp i olika aspekter och föreslås särskilda åtgärder för varje aspekt. Där så är lämpligt beskrivs även lyckade exempel.

De föreslagna åtgärderna är uppdelade enligt följande struktur:
- **Genomförande- och** verkställighetsåtgärder för framför allt stat och myndigheter, bland annat i fråga om korrigerande åtgärder och påföljder, klagomålsmekanismer, gränsöverskridande klagomål, samarbete med tredje land och övervakning (avsnitt 3).
- **Självreglering och tekniska åtgärder** för framför allt marknadsaktörer, bland annat i fråga om avtalsvillkor, yrkesetiska regler, godtagbara marknadsföringsmetoder, märkning, alternativa tvistlösningsmekanismer och tekniska lösningar, exempelvis i fråga om filter och säkerhet (avsnitt 4).
- **Åtgärder för ökad medvetenhet** om förebyggande åtgärder, konsumentutbildning, och rapporteringsmekanismer, att genomföras av stat och myndigheter, marknadsaktörer, konsumentorganisationer och liknande organ (avsnitt 5).

Åtgärderna sammanfattas i en tabell i slutet av meddelandet. Åtgärderna har olika inbördes kopplingar och bör i möjligaste mån genomföras parallellt och på ett integrerat sätt.

Längre ned redogörs för åtgärderna i detalj. Först analyseras dock begreppet skräppost som sådant (avsnitt 1) och påminns om de nya regler som gäller sedan den 31 oktober 2003 (avsnitt 2).

1. SKRÄPPOSTPROBLEMET

Vad är skräppost?

Begreppet skräppost används ofta utan att man gör klart för sig vad det egentligen betyder. Vad som avses är kort sagt icke begärd e-post, ofta i form av massutskick. Begreppet skräppost varken används eller definieras i det nya direktivet. I stället talas det om ”icke begärd kommunikation” via ”elektronisk post” ”för direkt marknadsföring”, vilket i praktiken omfattar all slags skräppost. I detta meddelande används därför skräppost som sammanfattande begrepp för icke begärd kommersiell elektronisk post.

Det bör påpekas att begreppet elektronisk post inte bara omfattar traditionell SMTP-baserad e-post utan också SMS, MMS och alla andra former av elektronisk kommunikation där avsändare och mottagare inte måste vara aktiva samtidigt (se avsnitt 2).

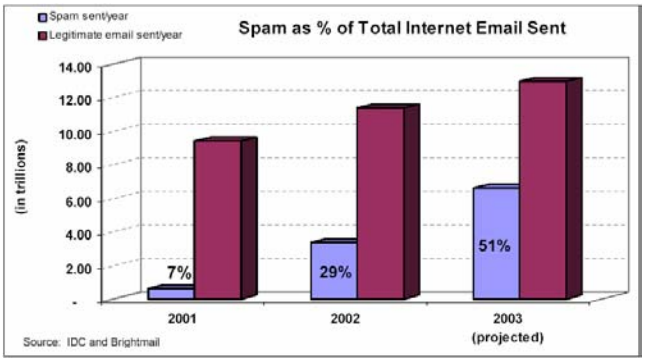
1.1. Problemets omfattning

Skräpposten har antagit oroväckande proportioner. De statistiska uppgifterna skiftar visserligen, men den allmänna uppskattningen är att över 50 % av den globala e-posttrafiken utgörs av skräppost.

---

arbetsgruppen för uppgiftsskydd. Med hjälp av en enkät samlades det in uppgifter från medlemmarna i COCOM och arbetsgruppen. Synpunkter kom också från en rad branschorganisationer och enskilda företag (allt från Internetleverantörer och operatörer av mobila och fasta kommunikationsnät, över masspostare och reklambyråer, till dator- och programtillverkare).

Ännu mer oroväckande är hastigheten med vilken denna andel ökar. Ännu 2001 uppskattades skräpposten ”bara” stå för 7 % av den globala e-posttrafiken. 2002 hade andelen ökat till 29 %. Enligt prognoserna uppskattas skräppostens andel 2003 uppgå till 51 %.



Figur 1: Skräppost som andel av all e-post på Internet

Det kan råda avsevärda skillnader mellan olika användargrupper och olika regioner i världen. (Vid Europeiska kommissionen uppskattas exempelvis 30 % av den externa e-posten bestå av skräppost.) Generellt är dock de senaste EU-siffrorna inte mindre oroväckande än de globala siffrorna[5].

Skräppost via mobilnät, t.ex. i form av textmeddelanden mellan mobiltelefoner (SMS), verkar för närvarande vara ett mindre problem, men nya tekniska lösningar, såsom e-post via mobiltelefoner, torde öka mängden skräppost. Att det rör sig om ett verkligt hot bekräftas av erfarenheterna i länder med utbredd I-mode-kommunikation (t.ex. Japan).

[5] Under september 2003 uppskattades skräppostens andel i EU uppgå till 49 %, jämfört med ungefär 54 % i hela världen under samma period (källa: Brightmail, 2003).

1.2. Vad gör skräppost till ett problem?

Ur den enskilda användarens synvinkel inkräktar skräpposten på integriteten. Det är främst detta som de nya reglerna om skräppost i nästa avsnitt handlar om. Skräppost innehåller dessutom ofta vilseledande eller försåtliga uppgifter. Avsikten bakom en stor del av skräpposten verkar vara att lura konsumenterna genom sådana uppgifter[6]. Tyvärr svarar alldeles för många konsumenter på dessa skräppostmeddelanden[7]. Dessutom kan meddelanden med pornografiskt innehåll vara stötande[8]. Att städa brevlådan för att bli av med skräppost tar ofta mycket tid, och om det behövs filter eller annan programvara ökar dessutom användarkostnaderna.

Är det någon som bryr sig?

Antalet klagomål ger en fingervisning om användarnas irritation. På tre månader kom det in 325 000 meddelanden till den franska e-postlådan för skräppostklagomål. Ett liknande försök i Belgien resulterade i 50 000 klagomål på 2,5 månader[1]. FTC:s permanenta e-postlåda för skräppostklagomål (den så kallade UCE-databasen) fylldes i början av 2003 med 130 000 meddelanden om dagen[1].

Skräpposten har nått en omfattning som också medför betydande kostnader för företagen. Direkta kostnader uppstår på grund av att de anställda måste städa i sina brevlådor och på så sätt blir mindre effektiva och produktiva. Företagens datoravdelningar lägger ned tid och pengar på att försöka lösa problemet. Internet- och e-postleverantörer måste köpa mer bandbredd och lagringskapacitet för oönskad e-post. Det finns också risk att skräpposten ställer till med problem för den som tar emot meddelandet (t.ex. skadligt innehåll på anställdas datorer) eller bara helt aningslöst vidarebefordrar det (t.ex. felaktig svartlistning, skadat rykte). Det kan också uppstå indirekta kostnader: Vissa legitima kommersiella eller affärsrelaterade e-postmeddelanden kommer inte fram på grund av den aktuella filtertekniken (så kallade falska positiva resultat) eller blir helt enkelt inte lästa för att de

---

6 Enligt en färsk rapport från FTC innehöll 22 % av den skräppost som analyserats felaktig information i rubriken. I 42 % av fallen var informationen i rubriken vilseledande och gav sken av att avsändaren stod i något affärsmässigt eller personligt förhållande till mottagaren. I 44 % av fallen var uppgifterna om avsändaren eller i rubriken felaktiga. I över hälften av all skräppost om finansiella frågor var uppgifterna om avsändaren eller i rubriken felaktiga. 40 % av all skräppost visade tecken på osanningar i meddelandet. 90 % av skräpposten om investerings- och affärsmöjligheter innehöll påståenden 66 % av skräpposten innehöll felaktiga uppgifter om avsändaren, i rubriken eller i meddelandet. (*False Claims in Spam, A report by the FTC's Division of Marketing Practices*, 30 april 2003, återfinns på http://www.ftc.gov/reports/spam/030429spamreport.pdf).

7 Enligt Pew Internet uppger 7 % av e-postanvändarna att de har gjort en beställning till följd av skräppost, och 33 % uppger att de har klickat på en länk i skräppostmeddelandet för att få mer information. Även om andelen konsumenter som lurats fortfarande är relativt låg, har problemet med konsumentbedrägerier nått helt nya nivåer på grund av de enastående stordriftsfördelar som bedragare kan uppnå med hjälp av vilseledande eller försåtlig skräppost. Se *Spam - How It Is Hurting Email and Degrading Life on the Internet, October 2003*, rapport av Deborah Fallows för Pew Internet & American Life Project. Rapporten återfinns på följande webbadress http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf. På FTC:s skräppostforum i april-maj 2003 intygade en masspostare att han skulle gå med vinst även om svarskvoten skulle ligga under 0,0001 %. (Kommentarer av Timothy J. Muris, FTC:s ordförande, Federal Trade Commission, vid ett möte i Aspen, Colorado, den 19 augusti 2003, ”Cyberspace and the American Dream, The Progress and Freedom Foundation”).

8 Skräpposten innehåller ibland också omotiverat våld eller uppmaningar till hets mot folkgrupp på grund av ras, kön, religion eller nationalitet.

förknippas med skräppost. Skräppost används också i ökande omfattning för att sprida virus, vilket kan skapa stora kostnader för företagen.

Det är svårt att mäta de kostnader som skräpposten orsakar, särskilt för enskilda användare, inte minst för att det delvis är svårt att sätta ett ekonomiskt värde på skadan. Uppskattningarna är dock generellt oroväckande. Bara i produktivitetsförluster uppskattar Ferris Research exempelvis att de europeiska företagens kostnader för skräppost 2002 uppgick till 2,5 miljarder euro[9]. Såsom redan nämnts har mängden skräppost ökat avsevärt sedan 2002. Programföretaget MessageLabs Ltd uppskattade i juni 2003 de brittiska företagens kostnader för skräppost till runt 3,2 miljarder pund sterling[10]. Beroende på vilken sektor som berörs kan skräpposten få olika följder. Inom rättssektorn kan skräpposten få särskilt stora konsekvenser med tanke på hur konfidentiella och känsliga de behandlade uppgifterna är.

En av skräppostens mest oroväckande följder är att den undergräver användarnas förtroende och därmed hindrar utvecklingen av e-handeln och informationssamhället som helhet. Seriösa affärsidkares anseende i en sektor kan ta stor skada, om man får intrycket av att ett återförsäljningsmedium utnyttjas av bedragare. De senaste siffrorna från Förenta staterna, som har mer erfarenhet av skräppost än EU, bekräftar att många människors förtroende för e-posten har minskat på grund av all skräppost de får[11].

Generellt förväntas Internet och annan elektronisk kommunikation – exempelvis bredband och trådlös kommunikation – på ett avgörande sätt bidra till produktivitetstillväxten i de moderna ekonomierna. Utan ordentliga säkerhetsåtgärder kan en del av de funktioner som gör tjänsterna så attraktiva – exempelvis ständig uppkoppling och trådlös åtkomst – också bidra till en avsevärd ökning av den mängd skräppost som tas emot. Utvecklingens skuggsida är att en ökad spridning av dessa tjänster skulle kunna leda till en ökad mängd skräppost om det inte snabbt vidtas effektiva åtgärder.

2. REGLERNA OM SKRÄPPOST I KORTHET

2.1. Opt-in-systemet

Enligt direktiv 2002/58/EG om integritet och elektronisk kommunikation (sista dag för genomförandet: 31 oktober 2003) skall medlemsstaterna förbjuda sändandet av icke begärda kommersiella e-postmeddelanden eller andra elektroniska meddelanden såsom SMS- och MMS-meddelanden, om inte abonnenten av de berörda elektroniska kommunikationstjänsterna i förväg har gett sitt samtycke (artikel 13.1 i direktivet)[12].

---

9 Källa: Ferris Research, 2003.

10 Denna siffra och andra uppskattningar nämns i ”'Spam'; Report of an Inquiry by the All Party Internet Group”, London, oktober 2003, s. 8. Rapporten återfinns på följande webbadress: http://www.apig.org.uk.

11 Enligt ovannämnda undersökning som Pew Internet nyligen genomförde använder 25 % av de intervjuade personerna e-posten mindre för att de får så mycket skräppost.

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

Detta är det så kallade opt-in-systemet som hittills bara har gällt för fax och automatisk uppringningsutrustning[13].

Tre grundregler i det nya systemet:

Regel nr 1: Abonnenten måste i förväg ha gett sitt samtycke till e-postreklam. Ett begränsat undantag gäller för e-postmeddelanden (eller SMS-meddelanden) som av samma person skickas till en befintlig kund och som gäller likartade tjänster eller produkter. Systemet gäller abonnenter som är fysiska personer, men medlemsstaterna kan utvidga det till att även omfatta juridiska personer.

Regel nr 2: Det är förbjudet att dölja eller hemlighålla identiteten på den avsändare för vars räkning meddelandet skickas.

Regel nr 3: Alla e-postmeddelanden måste innehålla en giltig returadress så att man kan meddela att man inte längre vill ha utskicket (opt-out).

All skräppost är dock inte förbjuden. Ett undantag gäller, om kontaktuppgifter för e-post- eller SMS-meddelanden har lämnats i samband med en försäljning. Detta kallas ibland ”soft opt-in”. Inom ett sådant befintligt kundförhållande får det företag som fått uppgifterna från kunden använda dessa uppgifter för att marknadsföra sådana produkter eller tjänster som liknar dem som företaget redan har sålt till kunden. Detta undantag har harmoniserats på gemenskapsnivå, och medlemsstaterna är skyldiga att tillämpa det. Det måste dock strikt begränsas så att man inte undergräver opt-in-systemet i praktiken. Även i så fall måste företaget emellertid redan då uppgifterna samlas in för första gången klargöra att de kan komma att användas för direkt marknadsföring (och att de i förekommande kan komma att lämnas ut till tredje part i samma syfte). Företaget bör dessutom ge kunden möjlighet att ”kostnadsfritt och enkelt” motsätta sig sådan användning. Vidare bör varje följande kommunikation för direkt marknadsföring ge kunden möjlighet att enkelt och kostnadsfritt meddela att man inte önskar få fler meddelanden (opt-out).

Opt-in-systemet är obligatoriskt för alla e-post- och SMS-meddelanden för direkt marknadsföring som är riktade till enskilda (fysiska) personer. Medlemsstaterna kan utvidga opt-in-systemet till att även omfatta kommunikationer till företag. De medlemsstater som redan tidigare hade infört ett opt-out-system för marknadsföring mellan företag, inklusive opt-out-register, kan behålla systemet. Ett system där man inom ramen för en e-posttjänst differentierar mellan abonnentgrupper kan medföra specifika problem för avsändaren när det gäller att skilja mellan juridiska och fysiska personer.

Oavsett mottagargrupp (juridiska eller fysiska personer) är meddelanden för direkt marknadsföring förbjudna enligt direktivet, om identiteten på avsändaren döljs eller hemlighålls. Sådana kommunikationer måste dessutom innehålla en giltig adress till vilken mottagaren kan skicka en begäran om att meddelandena skall upphöra[14].

Artikel 29-arbetsgruppen för uppgiftsskydd, som inrättades för att bistå kommissionen och som består av företrädare för EU:s dataskyddsmyndigheter, är i färd med att närmare

---

13 För andra reklamsamtal på taltelefon än från automatisk uppringningsutrustning får medlemsstaterna välja mellan opt-in och opt-out.

14 Artikel 13.4 i direktiv 2002/58/EG.

granska några av dessa lösningar för att bidra till en enhetlig tillämpning av nationella bestämmelser enligt direktiv 2002/58/EG[15].

Genom samförstånd i dessa frågor undviker man olika tolkningar som skulle skada den inre marknadens funktion. Andra frågor i samband med skräppost har tagits upp i tidigare dokument från arbetsgruppen[16].

2.2. Verkställighetsbestämmelser

Bestämmelserna om rättslig prövning, ansvar och sanktioner i det allmänna uppgiftsskyddsdirektivet 95/46/EG är också tillämpliga på bestämmelserna i direktivet om integritet och elektronisk kommunikation, inbegripet bestämmelserna om skräppost[17].

Kort sagt måste medlemsstaterna se till att det finns sanktioner och möjlighet till rättslig prövning om bestämmelserna inte följs. Var och en måste ha rätt att föra talan inför domstol om kränkningar av de rättigheter som skyddas av den nationella lagstiftningen. Denna rättsliga prövning får visserligen inte påverka möjligheten att (eventuellt först) utnyttja något administrativt förfarande, men det finns inga harmoniserade krav på att det skall finnas sådana administrativa förfaranden. Var och en som lidit skada till följd av olaga behandling av personuppgifter eller en otillåten gärning måste ha rätt till ersättning. Om någon överträder bestämmelserna, måste man kunna tillgripa sanktioner för att se till att direktivet genomförs fullt ut.

Direktivets särart innebär med andra ord att medlemsstaterna visserligen har ett visst handlingsutrymme när det gäller valet av åtgärder för att genomföra direktivet, även i fråga om korrigerande åtgärder och påföljder, men att de måste se till att bestämmelserna om skräppost ”genomförs fullt ut”.

---

15 I enlighet med artikel 15.3 i direktiv 2002/58/EG jämförd med artikel 30 i direktiv 95/46/EG.

16 Se exempelvis yttrande 7/2000 om Europeiska kommissionens förslag till Europaparlamentets och rådets direktiv om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation av den 12 juli 2000; rekommendation 2/2001 om vissa minimikrav för insamling av personuppgifter på Internet inom Europeiska unionen; okontrollerad insamling av personuppgifter diskuteras i arbetsdokumentet av den 21 november 2000 om ”Skydd av privatlivet på Internet - Ett integrerat förhållningssätt till dataskydd på Internet”. Dokumenten återfinns på följande webbadress: http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm

17 Artikel 15 i direktiv 2002/58/EG innehåller en hänvisning till kapitel III i direktiv 95/46/EG, som gäller rättslig prövning, ansvar och sanktioner:
Artikel 22 – Rättslig prövning
Medlemsstaterna skall - utan att det påverkar möjligheten att utnyttja något administrativt förfarande, till exempel vid den tillsynsmyndighet som avses i artikel 28, som kan användas innan ett ärende anhängiggörs hos en rättslig instans - föreskriva att var och en har rätt att föra talan inför domstol om sådana kränkningar av rättigheter som skyddas av den nationella lagstiftning
Artikel 23 – Ansvar
1. Medlemsstaterna skall föreskriva att var och en som lidit skada till följd av en otillåten behandling av personuppgifter eller av någon annan åtgärd som är oförenlig med de nationella bestämmelser som antagits till följd av detta direktiv, har rätt till ersättning av den registeransvarige för den skada som han har lidit.
2. Den registeransvarige kan helt eller delvis undgå detta ansvar om han bevisar att han inte är ansvarig för den händelse som orsakade skadan.
Artikel 24 – Sanktioner
Medlemsstaterna skall anta lämpliga bestämmelser för att säkerställa att detta direktiv genomförs fullständigt och skall särskilt besluta om de sanktioner som skall användas vid överträdelse av de bestämmelser som antagits för att genomföra detta direktiv.

Såsom det brukar vara när det gäller direktiv är det i första hand medlemsstaterna som ansvarar för verkställandet, inte kommissionen.

Det är alltså inte kommissionens uppgift att åtala eller bötfälla dem som bryter mot direktivets bestämmelser om rättigheter och skyldigheter[18].

2.3. Övriga bestämmelser om skräppost

I samband med skräppostandet sker ofta okontrollerad insamling av e-post-relevanta uppgifter, dvs. automatisk insamling av personuppgifter på offentliga platser på Internet, t.ex. webbplatser och chattlinjer. Enligt det allmänna uppgiftsskyddsdirektivet 95/46/EG är sådan insamling förbjuden, oavsett om den sker automatiskt med hjälp av ett program eller inte[19].

Bedräglig och försåtlig skräppost är särskilt obehaglig. Enligt befintliga EU-regler om vilseledande reklam och otillbörliga affärsmetoder är sådana affärsmetoder redan förbjudna (t.ex. direktiv 84/450/EEG om vilseledande reklam)[20]. För allvarligare fall föreskrivs i nationell lagstiftning dessutom strängare, även straffrättsliga, påföljder.

Vissa slag av skräppost kan vara ännu mer stötande, exempelvis meddelanden med pornografiskt innehåll eller omotiverat våld, särskilt om det är barn som utsätts för dem[21]. Visserligen behöver innehållet som sådant inte vara otillåtet, även om det kan vara skadligt, men enligt nationell lagstiftning är urskiljningslös spridning bland vuxna och barn normalt förbjuden, ibland med hot om relativt stränga straff. Skräppostens innehåll kan också vara otillåtet, såsom uppmaning till hets mot folkgrupp på grund av ras, kön, religion eller nationalitet. I den mån sådana meddelanden används för direkt marknadsföring – vilket ofta är fallet – omfattas de under alla omständigheter av skräppostförbudet, liksom andra slag av skräppost.

Enligt artikel 6 a direktivet om elektronisk handel skall ”det kommersiella meddelandet” vara klart identifierbart som sådant (direktiv 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden)[22].

---

18 I motsats till exempelvis Förenta staternas ”Federal Trade Commission”.

19 Se även det arbetsdokument som utarbetats av artikel 29-arbetsgruppen för uppgiftsskydd och som gäller ”Skydd av privatlivet på Internet - Ett integrerat förhållningssätt till dataskydd på Internet” (dokument nr WP 37, antaget den 21 november 2000).

20 Rådets direktiv 84/450/EEG av den 10 september 1984 om tillnärmning av medlemsstaternas lagar och andra författningar om vilseledande reklam, EGT L 250, 19.9.1984, s. 17–20. Kommissionen lade nyligen fram ett förslag om ändring av direktivet om vilseledande reklam [KOM(2003) 356 slutlig].

21 Den 24 september 1998 antog rådet rekommendationen om utvecklingen av konkurrenskraften hos den europeiska industrin för audiovisuella tjänster och informationstjänster genom främjande av nationella system för att uppnå en jämförbar och effektiv skyddsnivå för minderåriga och för den mänskliga värdigheten (98/560/EG). Rekommendationen var det första rättsliga instrumentet på EU-nivå som gällde audiovisuella tjänsters och informationstjänsters innehåll och som omfattade alla former av tillhandahållande, från radio/TV till Internet.

22 Europaparlamentets och rådets direktiv av den 8 juni 2000, EGT L 178, 17.7.2000. I allmänhet måste ett ”kommersiellt meddelande” följa gällande regler i den medlemsstat där tjänsteleverantören är etablerad. Detta gäller dock inte frågan om huruvida icke begärd kommunikation via e-post är tillåten (se artikel 3 i direktivet om elektronisk handel och bilagan till det direktivet). I de (begränsade) fall där fysiska personer inte skyddas mot skräppost genom direktiv 2002/58/EG (t.ex. fysiska personer som inte är abonnenter) måste medlemsstaterna enligt direktivet om elektronisk handel se till att tjänsteleverantörer som sänder icke begärda

I skräppostandets kölvatten begås också brott som hackning och identitetsstöld för att göra det möjligt att skicka skräppost eller få tillgång till databaser, adresser eller datorer. Sådan verksamhet kommer till stor del att omfattas av rambeslutet om angrepp mot informationssystem och på så sätt beläggas med straffrättsliga påföljder. Rambeslutet, om vilket det i februari 2003 uppnåddes politisk enighet och som bygger på ett förslag från kommissionen, torde snart bli officiellt antaget[23]. Redan i dag kan olaga intrång på servrar eller datorer eller missbruk av datorer i många medlemsstater åtalas som brott.

3. EFFEKTIVT GENOMFÖRANDE OCH VERKSTÄLLANDE I MEDLEMSSTATERNA OCH GENOM MYNDIGHETER

I detta avsnitt om effektivt genomförande och verkställande föreslås åtgärder för framför allt stat och myndigheter i fråga om korrigerande åtgärder och påföljder, klagomålsmekanismer, gränsöverskridande klagomål, samarbete med tredje land och övervakning.

Inledningsvis bör påpekas att en rad medlemsstater ännu inte har införlivat direktivet om integritet och elektronisk kommunikation, som även omfattar bestämmelser om skräppost och som är ett led i ett nytt och mer allmänt regelverk för elektronisk kommunikation[24]. Europaparlamentet uttryckte nyligen sin oro över denna försening[25]. Eftersom direktivet om integritet och elektronisk kommunikation senast skulle ha införlivats den 31 oktober 2003, inledde kommissionen i november 2003 överträdelseförfaranden mot flera medlemsstater som inte hade anmält några genomförandeåtgärder[26].

3.1. Inledning

Lagstiftning kan delvis förhindra skräppost men är inte tillräcklig. Alla medlemsstater måste prioritera opt-in-systemets verkställande. Vid sidan om tillräcklig personal och tillräckliga resurser betyder det att man behöver lämpliga verkställighetsmekanismer, även när det gäller verkställighet över gränserna. Samarbetet med länder utanför EU är också viktigt. Lika viktigt är det att övervaka verkställandet, åtminstone för att fastställa prioriteringar.

Följande faktorer torde påverka verkställighetsmekanismernas effektivitet:

– Möjligheten att se till att lagstiftningen följs med hjälp av effektiva böter eller andra påföljder. En rad tillsynsmyndigheter saknar uppenbarligen fortfarande (effektiva) befogenheter att ingripa.

---

kommersiella meddelanden per e-post regelbundet konsulterar och respekterar de opt-out-register där fysiska personer som inte önskar erhålla sådana kommersiella meddelanden kan registrera sig (se artikel 7 i direktivet om elektronisk handel).

23 Förslag till rådets rambeslut om angrepp mot informationssystem, KOM(2002) 173 slutlig av den 19 april 2002.

24 Se även nionde rapporten om genomförandet av EU:s lagstiftning på telekommunikationsområdet, som återfinns på följande webbadress: http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/annualreports/9threport/index_en.htm

25 Betydelsen av ett fullständigt, effektivt och snabbt genomförande av det nya regelverket för elektronisk kommunikation, inklusive detta direktiv, har kommissionen lyft fram i sitt meddelande ”Elektronisk kommunikation: Vägen till den kunskapsbaserade ekonomin” (KOM(2003) 65 av den 11 februari 2003).

26 De formella underrättelserna skickades den 25 november 2003 (se IP/03/1663).

– Vilka slags klagomålsmekanismer och korrigerande åtgärder som enskilda personer och företag kan åberopa.

– Behovet av klarhet och samordning i fråga om de nationella myndigheternas skyldigheter på området, eftersom de delvis överlappar varandra.

– Graden av medvetenhet bland användarna om vilka rättigheter de har och hur de kan göras gällande. Användarna måste informeras om var de skall klaga, vad som kommer i fråga för en undersökning, vilka verkställighetsåtgärder som eventuellt kommer att vidtas och vilka upplysningar som krävs för att myndigheterna skall kunna inleda en undersökning.

– Samordning och samarbete mellan medlemsstaterna och mellan medlemsstaterna och tredje land för att avgöra vilket lands lagstiftning som skall gälla i ett specifikt fall.

– Tillgängliga resurser för spårning av de skräppostare inom eller utanför EU som döljer sin identitet eller använder andra användares identitet, adresser eller servrar.

Vad som gäller för bestämmelserna om skräppost i fråga om verkställighet förklaras närmare i avsnitt 2.2. Hittills har skräppostproblemet hanterats på mycket olika sätt[27]. Visserligen innebär ett EU-direktiv som rättsligt instrument att medlemsstaterna har ett visst handlingsutrymme när det gäller direktivets genomförande, men oberoende av vilken metod som tillämpas måste de se till att bestämmelserna verkligen efterlevs.

[27] Det bör noteras att klagomål ofta också gäller skräppostrelaterade frågor, såsom rätten att få tillgång till personuppgifter och rätten att motsätta sig behandling av uppgifter.

Skillnader mellan medlemsstaterna

Det är inte samma myndighet i alla medlemsstater som ser till att bestämmelserna om skräppost efterlevs. I de flesta länder är det främst dataskyddsmyndigheten som övervakar efterlevnaden. I några länder är det däremot den nationella tillsynsmyndigheten för elektronisk kommunikation som har denna uppgift. I vissa länder är det i stället främst konsumentskyddsmyndigheter, exempelvis konsumentombudsmannen, som ser till att reglerna följs. Ofta är flera myndigheter inblandade. Dessutom är skräppost ofta liktydig med vilseledande budskap och bedrägeri. (I en minoritet av medlemsstaterna som saknar konsumentskyddsmyndighet är det upp till konsumentorganisationer eller konsumenterna själva att se till att bestämmelserna följs.) Skräppostandet är ofta kopplat till överträdelse av dataskyddsbestämmelser, t.ex. okontrollerad insamling av personuppgifter, eller IT-brottslighet, t.ex. olaga intrång i datorer eller servrar. Efterlevnaden av de relevanta bestämmelserna övervakas eventuellt inte av samma myndighet, särskilt inte när det gäller gränsöverskridande överträdelser.

Utom i några få medlemsstater leder klagomål inte nödvändigtvis till en undersökning. Med viss framgång knyts ibland kontakter innan något förfarande inleds, exempelvis genom att man ger företag riktlinjer och vägledningar. Ibland är det konsumenten själv som förväntas ta kontakt med företaget innan ett klagomål lämnas in. Vissa länder (t.ex. Förenade kungariket) har infört självreglering som första åtgärdsfas. I en rad länder har näringslivet redan infört självreglerande klagomålsmekanismer. Även myndigheterna agerar ofta på eget initiativ. Att en myndighet är inkopplad innebär normalt inte att man inte längre kan gå direkt till domstol.

Inte alla dataskyddsmyndigheter har behörighet att vidta åtgärder mot juridiska personer. De har (än så länge) inte heller alltid möjlighet att tillgripa sanktioner. I stället måste de väcka talan vid domstol. I Frankrike såg sig dataskyddsmyndigheten föranledd att lägga fram några utvalda fall för de rättsliga myndigheterna, utan någon större framgång. Ett liknande fall i Belgien ledde till ett meningsutbyte med de misstänkta avsändarna. Gränsöverskridande fall har lämnats till myndigheterna i de berörda medlemsstaterna eller till amerikanska FTC.

Ett välavvägt tillvägagångssätt som omfattar både lagstiftning, verkställighetsåtgärder och självreglering anses allmänt vara den bästa metoden för att omsätta opt-in-systemet i praktiken. Medlemsstaterna uppmanas undersöka hur effektiva deras verkställighetsmekanismer är, särskilt mot bakgrund av nedan föreslagna åtgärder (se avsnitten 3.2–3.6).

Medlemsstaterna uppmanas också ta fram nationella strategier för att få dataskyddsmyndigheter, konsumentskyddsmyndigheter och nationella tillsynsmyndigheter för e-kommunikation att samarbeta så att man undviker dubbelarbete och överlappning av verksamheter.

För att underlätta och samordna utbyte av information om och lyckade exempel på effektiva åtgärder som vidtagits för att se till att reglerna följs (t.ex. när det gäller klagomål, korrigerande åtgärder, påföljder och internationellt samarbete) har kommissionen, med medlemsstaternas och dataskyddsmyndigheternas stöd, tillsatt en **informell och nätbaserad skräppostgrupp**. Gruppen kommer också att underlätta och samordna arbetet på andra åtgärdsområden som tas upp i detta meddelande, exempelvis i fråga om ökad medvetenhet och tekniska lösningar.

För att man skall kunna vidta lämpliga åtgärder kommer de dokument som bygger på diskussioner i gruppen generellt att överlämnas till kommunikationskommittén (COCOM), inrättad inom ramen för regelverket för elektroniska kommunikationsnät och kommunikationstjänster, och/eller till artikel 29-arbetsgruppen för uppgiftsskydd.

Gruppen kan bland annat komma att utarbeta benchmarkingkriterier för olika åtgärdsförslag.

Gruppen består bland annat av företrädare för behöriga nationella förvaltningar, dataskyddsmyndigheter och kommissionen. Gruppen kommer att utreda hur man kan få andra berörda parter att medverka.

3.2. Effektiva korrigerande åtgärder och påföljder

3.2.1. Bakgrund

För närvarande utgörs de korrigerande åtgärderna mest av böter och förelägganden om att man skall upphöra med den olaga databehandlingen, ibland också blockering av de berörda webbplatserna. I några medlemsstater är dessa förelägganden kopplade till böter (t.ex. om föreläggandet inte beaktas). Alla myndigheter har dock inte behörighet för alla slag av skräppostrelaterade överträdelser och har heller inte tillgång till samma instrument. Fallen hänskjuts ofta till rättsliga myndigheter. Alla medlemsstater har inte infört rättsliga påföljder för överträdelser.

Alla medlemsstater har inte infört korrigerande åtgärder och böter/påföljder i sin förvaltningsrätt respektive straffrätt. De straffrättsliga påföljderna varierar. I vissa medlemsstater kan det utdömas fängelsestraff. Dessutom kan man normalt begära civilrättsligt skadestånd.

Visserligen görs det ofta skillnad mellan lindriga och allvarliga brott (t.ex. skräppostande i stor skala, vilseledande reklam och bedrägeri), men påföljderna varierar avsevärt mellan medlemsstaterna.

I många fall leder skräppostandet också till korrigerande åtgärder enligt allmän dataskyddslagstiftning (t.ex. överträdelser när det gäller anmälningsplikt, rätt till tillgång och skyldighet att utnämna en företrädare i en medlemsstat) eller särskild lagstiftning (t.ex. vilseledande reklam och bedrägerier). Innan opt-in-systemet infördes tillämpades olika rättsliga åtgärder för att få bukt med vissa slag av skräppost (t.ex. massutskick, olaga användning av personuppgifter, nätstörningar, missbruk av e-postadresser, bedrägeri och feltolkning av avtal).

Enligt den allmänna uppfattningen räcker rättslig prövning inte för att se till att reglerna följs. Normalt kan dataskyddsmyndigheter, konsumentskyddsmyndigheter och nationella tillsynsmyndigheter fastställa böter, men beloppen varierar. De flesta medlemsstater där detta ännu inte är möjligt överväger att införa böter. För en så dynamisk sektor som denna verkar administrativa sanktioner vara lämpligare än rättslig prövning. Dataskyddsmyndigheter, konsumentskyddsmyndigheter och nationella tillsynsmyndigheter begagnar sig ofta av kompletterande instrument för att se till att reglerna följs. Administrativa förfaranden kan vara både billiga och snabba (enligt uppgift från den italienska dataskyddsmyndigheten exempelvis 50 dagar).

3.2.2. Föreslagna åtgärder

Först och främst uppmanar kommissionen de medlemsstater som ännu inte har gjort det att omgående införliva direktivet med sin lagstiftning, i synnerhet bestämmelserna om skräppost. Vid behov är kommissionen beredd att bistå medlemsstaterna i detta.

Medlemsstaterna uppmanas undersöka hur effektiva deras system för korrigerande åtgärder och påföljder är när det gäller överträdelser. De uppmanas vidare att införa lämpliga skadeståndsmöjligheter för dem som drabbas.

De medlemsstater och behöriga myndigheter som saknar administrativa förfaranden bör överväga att införa sådana förfaranden mot skräppost för att på ett snabbt, billigt och effektivt sätt se till att opt-in-systemet följs.

Kommissionen kommer att förvissa sig om att de nationella genomförandeåtgärderna leder till kännbara sanktioner, vid behov även ekonomiska och straffrättsliga, om marknadsaktörerna inte uppfyller sina skyldigheter.

I detta sammanhang kommer kommissionen också att undersöka i vilken mån de behöriga myndigheterna kan undersöka och ingripa.

3.3. Klagomålsmekanismer

3.3.1. Bakgrund

För att man skall kunna se till att reglerna följs måste det finnas lämpliga klagomålsmekanismer. En rad dataskyddsmyndigheter har infört e-postlådor dit användarna kan vidarebefordra skräppost, och myndigheterna har åtagit sig att vidta åtgärder i specifika fall.

Vissa medlemsstater genomför hellre normala administrativa förfaranden eller tar vid nätstörningar kontakt med Internetleverantörerna eller privata grupper för stöd vid datorhaveri (*Computer Emergency Response Team*, CERT). Andra medlemsstater tillämpar hellre mer traditionella förfaranden (civilrättsliga skadeståndsmål eller administrativa förfaranden). Ibland lämpar sig sam- eller självreglering bättre än direkta verkställighetsåtgärder.

Lyckade exempel

Frankrike och Belgien har sedan slutet av 2002 haft särskilda e-postlådor för skräppostklagomål och fått mycket intressanta resultat. Rapporterna om dessa initiativ är offentliga[28]. Frankrike kommer troligtvis att ha en permanent sådan e-postlåda inom ramen för de nya regler som införs för att genomföra direktivet om integritet och elektronisk kommunikation. Förenta staternas *Federal Trade Commission* har en liknande postlåda som används för åtal enligt gällande lagar i fråga om otillbörliga och försåtliga affärsmetoder[29].

En fördel med e-postlådor för skräppostklagomål är att de uppmuntrar konsumenterna att rapportera överträdelser, vilket gör det lättare att se till att gällande lagstiftning följs. Man får dessutom viktiga statistiska uppgifter som ger en god överblick över hur stora ett lands eller en regions problem är och hur de är beskaffade, vilket i sin tur gör det lättare för myndigheterna att se vilka verkställighetsåtgärder som måste prioriteras eller

---

28 Den franska dataskyddsmyndighetens (*Commission National Informatique et Libertés*, CNIL) rapport av den 24 oktober 2002 återfinns på följande webbadress: http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm Den belgiska dataskyddsmyndighetens (*Commission de Protection de la Vie Privée*) rapport från juli 2003 återfinns på följande webbadress: http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf.

29 Se exempelvis http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf. Oönskade eller försåtliga meddelanden kan vidarebefordras till följande webbadress: uce@ftc.gov.

anpassas. De kan dessutom läggas till grund för förebyggande åtgärder. Den franska dataskyddsmyndigheten CNIL har exempelvis använt uppgifterna från sitt initiativ med en e-postlåda för skräppostklagomål för att ta fram förebyggande informationspaket för användare och reklambyråer som använder direkt marknadsföring, dvs. masspostare.

Hur väl en e-postlåda för skräppostklagomål lämpar sig för att övervaka och mäta skräppostens spridning och omfattning beror förstås på hur effektivt och snabbt man kan undersöka klagomålen.

Visserligen finns det ett utbrett intresse för att lära sig av andra medlemsstaters erfarenheter av e-postlådor för skräppostklagomål, men bara få medlemsstater planerar eller överväger att själva använda sådana e-postlådor. Som skäl anges oftast att man redan kan klaga med hjälp av e-post, vanligtvis på myndighetens webbplats, att det för en sådan e-postlåda krävs ytterligare personal och utrustning eller att man först måste ändra befintliga rättsliga förfaranden.

3.3.2. Föreslagna åtgärder

Medlemsstaterna och de behöriga myndigheterna bör undersöka hur effektivt deras rättssystem är när det gäller hanteringen av klagomål från användarna. Rättssystemen bör vid behov anpassas.

Medlemsstaterna och de behöriga myndigheterna uppmanas införa särskilda e-postlådor för skräppostklagomål kompletterade med informationskampanjer.

Dessa särskilda e-postlådor måste vara utformade så att de möjliggör enkel sökning och analys, ökar förståelsen av problemet och gör det lättare att prioritera verkställighetsåtgärder.

Kommissionen kommer att underlätta spridningen av de erfarenheter som görs med sådana e-postlådor.

3.4. Gränsöverskridande klagomål och verkställighetssamarbete inom EU

3.4.1. Bakgrund

En effektiv hantering av gränsöverskridande klagomål är ett led i ett effektivt konsumentskydd på området. För en effektiv handläggning av klagomål från användare i en medlemsstat när det gäller skräppost från en annan medlemsstat är det mycket viktigt att man, oberoende av förutsättningarna, kan koppla de olika nationella klagomålsmekanismerna till varandra (se punkt 3.5 för samarbete med tredje land).

Formella förfaranden för handläggning av gränsöverskridande klagomål saknas för närvarande i en rad medlemsstater. För närvarande löser man detta bland annat genom att hålla kontakt med den andra medlemsstatens relevanta myndighet och eventuellt hänskjuta klagomålet till den relevanta myndigheten i den medlemsstat där skräpposten har sitt ursprung.

För närvarande utbyter de europeiska dataskyddsmyndigheterna (även myndigheterna i EES- och kandidatländerna) information om gränsöverskridande klagomål med hjälp av den arbetsgrupp för handläggning av klagomål som inrättades inom ramen för de europeiska dataskyddschefernas konferens.

Den kan åberopas när det gäller gränsöverskridande klagomål om skräppost, bland annat för att utreda vilken lag som är tillämplig i ett visst fall. Inte alla dataskyddsmyndigheter ser emellertid till att bestämmelserna om skräppost följs.

På konsumentskyddsområdet föreslog kommissionen nyligen en förordning om konsumentskyddssamarbete genom upprättande av ett nät mellan konsumentskyddsmyndigheterna för att hantera gränsöverskridande problem[30]. Förordningen gäller förfaranden för ömsesidigt bistånd och fördjupat praktiskt samarbete mellan nationella myndigheter. Enligt förslaget skall systemet omfatta skräppost som är vilseledande eller försåtlig eller som bryter mot andra konsumentskyddsregler, men inte all skräppost som förbjuds genom direktivet om integritet och elektronisk kommunikation. Förordningen diskuteras för närvarande i rådet och parlamentet.

3.4.2. Föreslagna åtgärder

Medlemsstaterna och de behöriga myndigheterna uppmanas undersöka hur effektiva deras förfaranden för handläggning av gränsöverskridande klagomål är (t.ex. avtal om ömsesidigt bistånd).

Samordning mellan de behöriga nationella myndigheterna uppmuntras. Med detta avses bland annat samordning och utbyte av information mellan de myndigheter som verkställer nya bestämmelser och mellan dem och andra myndigheter med ansvar för specifika slag av skräppost (t.ex. skräppost med bedrägligt eller pornografiskt innehåll eller skräppost om olaga försäljning av hälsovårdsprodukter).

Rådet och parlamentet uppmanas att så snart som möjligt enas om den föreslagna förordningen om konsumentskyddssamarbete för att se till att EU:s konsumentskyddsmyndigheter är rustade för kampen mot bedräglig och försåtlig skräppost. De uppmanas också överväga en eventuell utvidgning av förordningens räckvidd till att även omfatta direktivet om integritet och elektronisk kommunikation.

Medlemsstaterna uppmanas undersöka hur man kan undanröja befintliga hinder mot informationsutbyte och samarbete och vad det finns för möjligheter att kräva åtgärder från myndigheter i andra medlemsstater. I praktiken skulle det eventuellt vara bra med en samordningsmekanism (se dataskyddsmyndigheternas ovannämnda initiativ) för samarbete mellan de nationella tillsynsmyndigheterna när det gäller verkställande av lagar över gränserna. Ett nätverk till stöd för samarbetet skulle kunna bygga på kommissionens befintliga program, exempelvis IDA-programmet[31].

Kommissionen avser att underlätta och främja de behöriga nationella myndigheternas samarbete, bland annat med hjälp av den nyligen tillsatta informella och nätbaserade skräppostgruppen. Kommissionen har i samarbete med medlemsstaterna och nationella verkställighetsmyndigheter börjat undersöka vilka konkreta åtgärder som krävs för att förbättra handläggningen av gränsöverskridande klagomål. Diskussionerna med de nationella myndigheterna kommer att fortsätta under hela 2004.

---

30 KOM(2003) 443 slutlig.

31 Information om IDA-programmet återfinns på följande webbadress: http://europa.eu.int/comm/enterprise/ida/index.htm

3.5. Samarbete med tredje land

3.5.1. Bakgrund

De nya reglerna är tillämpliga på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät i EU (och EES). Till följd av detta gäller artikel 13 i direktiv 2002/58/EG (opt-in-regeln) för all skräppost som tas emot på eller skickas från nät i EU (och EES). Det innebär att även meddelanden från tredje land måste följa EU-reglerna, liksom meddelanden med ursprung i EU som skickas till tredje land.

När det gäller meddelanden från tredje land kommer det förstås att vara mycket svårare att se till att regeln följs än när det gäller meddelanden från EU. Likväl är detta viktigt, eftersom en stor mängd skräppost kommer från länder utanför EU.

Det kommer visserligen att krävas en blandning av olika instrument (bland annat förebyggande åtgärder, filter, självreglering, avtal och internationellt samarbete), men detta avsnitt handlar främst om internationellt samarbete. Det internationella samarbetet måste främst syfta till att få länderna utanför EU att anta effektiv lagstiftning. Det andra målet är att samarbeta med tredje land för att se till att reglerna verkligen följs.

Det finns inte mycket erfarenhet av att genomdriva gällande opt-in- respektive opt-out-regler när det gäller meddelanden från länder utanför EU. Bortsett från att skräppost är ett relativt nytt fenomen, möter arbetet i första hand följande hinder: det är svårt eller ytterst mödosamt att identifiera skräppostens avsändare; det saknas (lämpliga) mekanismer för internationellt samarbete; en del myndigheter har inte tillräckliga befogenheter i internationella frågor.

När det gäller bedräglig eller försåtlig skräppost innehåller kommissionens förslag till en förordning om konsumentskyddssamarbete också bestämmelser om samarbete med tredje land för att se till att reglerna följs. Organisationen för ekonomiskt samarbete och utveckling (OECD) antog 2003 en rekommendation för att skydda konsumenterna mot bedrägliga och försåtliga gränsöverskridande affärsmetoder[32].

3.5.2. Föreslagna åtgärder

En rad medlemsstater medverkar redan aktivt i multilaterala fora såsom OECD, där arbetet i fråga om skräppost redan har börjat. Ett aktivt deltagande i detta arbete uppmuntras särskilt för att hitta lösningar på internationell nivå.

Kommissionen kommer att arrangera en OECD-workshop om skräppost i februari 2004 som syftar till att öka förståelsen av skräppostproblemet och bidra till lösningar på internationell nivå. Workshopens resultat kommer att ligga till grund för konkreta uppföljningsåtgärder på OECD-nivå. Kommissionen diskuterar för närvarande dessa uppföljningsåtgärder med medlemsstaterna.

---

[32] *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* (”OECD:s riktlinjer för att skydda konsumenterna mot bedrägliga och försåtliga gränsöverskridande affärsmetoder”), OECD, 2003.

Åtgärderna omfattar bland annat arbete inom OECD för att främja effektiv lagstiftning på internationell nivå, ökad medvetenhet, tekniska lösningar, självreglering och internationellt samarbete för att se till att reglerna följs.

På FN-nivå framhålls i deklarationen från världstoppmötet om informationssamhället (Genève, 10–12 december 2003) och i den tillhörande handlingsplanen att skräppost bör bekämpas på lämplig nationell och internationell nivå. Kommissionen kommer att undersöka hur man bäst kan följa upp resultaten från 2003 års världstoppmöte i EU, med hänsyn tagen till toppmötet i Tunis 2005.

Medlemsstaterna och de behöriga myndigheterna uppmanas att stärka respektive inleda bilateralt samarbete med tredje land. Till detta hör inte bara främjande av effektiv lagstiftning utan också samarbete när det gäller reglernas genomdrivande, vid behov genom polissamarbete och rättsligt samarbete.

Myndigheterna uppmuntras också att samarbeta med den privata sektorn, inte minst med Internet- och e-postleverantörer, för att spåra skräppostare – förutsatt att det finns lämpliga rättsliga garantier.

Kommissionen kommer även fortsättningsvis att engagera sig i internationella fora, bland annat inom OECD och i den workshop som kommissionen arrangerar i Bryssel i februari 2004. Kommissionen kommer att fortsätta att hålla bilaterala möten och föra diskussioner med länder utanför EU, bland annat för att få dem att vidta effektiva åtgärder mot skräppost, särskilt när det gäller de mest obehagliga formerna av skräppost, och för att främja samarbete när det gäller reglernas genomdrivande.

Kommissionen har i samarbete med medlemsstaterna och nationella verkställighetsmyndigheter börjat undersöka hur man bäst sörjer för internationellt samarbete, särskilt när det gäller handläggning av klagomål om skräppost från tredje land. Arbetet med de nationella myndigheterna kommer att fortsätta under hela 2004.

3.6. Övervakning

3.6.1. Bakgrund

För att kunna bedöma hur opt-in-systemet fungerar i praktiken och för att lösa specifika problem med hjälp av lämpliga åtgärder behöver medlemsstaterna objektiva och aktuella uppgifter om skräppostens utveckling, om klagomål från användarna och om de svårigheter som tjänsteleverantörerna möter. Det handlar bland annat om följande informationskällor och informationsslag: utvecklingen när det gäller skräppostens karaktär, ursprung och volym av den skräppost som upptäcks av leverantörer av filterprogram, av tjänsteleverantörer och inom ramen för nationella (tillsyns-) initiativ samt, i förekommande fall, statistiska uppgifter från e-postlådor för skräppostklagomål.

OECD började 2003 att mäta skräppostens omfattning på internationell nivå och kommer att fortsätta sitt arbete under 2004.

Enligt artikel 18 i direktivet om integritet och elektronisk kommunikation skall det 2006 utarbetas en rapport om direktivets tillämpning och dess inverkan på ekonomiska aktörer och konsumenter, särskilt med avseende på icke begärda kommunikationer. För att kunna utarbeta denna rapport kommer kommissionen att behöva uppgifter från medlemsstaterna, bland annat relevant statistik.

3.6.2. Föreslagna åtgärder

Medlemsstaterna bör se till att de får den information och de statistiska uppgifter de behöver för att se till att reglerna följs, i förekommande fall i samarbete med näringslivet och med hänsyn till OECD:s pågående mätning av skräppostens omfattning.

Kommissionen kommer att utnyttja den nyligen tillsatta informella och nätbaserade skräppostgruppen för att underlätta och samordna utbyte av information om lyckade exempel, skräppostens utveckling och statistiska uppgifter om skräppost.

4. TEKNISKA ÅTGÄRDER OCH SJÄLVREGLERING INOM NÄRINGSLIVET

I detta avsnitt föreslås självregleringsåtgärder och tekniska lösningar för framför allt marknadsaktörer, bland annat i fråga om avtalsvillkor, yrkesetiska regler, godtagbara marknadsföringsmetoder, märkning och alternativa tvistlösningsmekanismer. Avsnittet handlar också om tekniska lösningar, exempelvis i fråga om filter och nätsäkerhet.

4.1. Effektiv tillämpning av opt-in-systemet

4.1.1. Bakgrund

Alla berörda parter måste engagera sig i kampen mot skräppost. Näringslivet kan spela en särskild roll genom att göra opt-in-systemet till normal praxis inom sin affärsverksamhet. Detta gäller inte bara slutanvändarnas affärsvillkor utan också relationerna till andra företag.

I många fall finns det behov av bättre samordning genom branschorganisationer och av medverkan från branschspecifika självregleringsorgan och konsument- och användarorganisationer, inklusive dataskyddsmyndigheter och andra behöriga nationella myndigheter.

Lyckade exempel

Sedan 2002 arrangerar exempelvis den nederländska plattformen för elektronisk handel ett forum för ”grundläggande principer för e-handeln”, där olika branscher (masspostare och Internetleverantörer) möter den nederländska konsumentorganisationen. Syftet är att omsätta opt-in-principen i praktiken. Den praktiska tillämpningen provas i samarbete med dataskyddsmyndigheten[33].

Avtal kan bidra till kampen mot skräppost, förutsatt att enskilda personers rättigheter skyddas. Många Internet- och e-postleverantörer har i sina kundavtal redan infört villkor enligt vilka det är förbjudet att använda tjänsterna för att sända skräppost. De förbjuder sändandet av icke begärd e-post eller masspost från sina e-postkonton[34].

De lösningar som Internetleverantörerna hittills har använt i sina kundavtal torde avvika från lösningarna i det nya direktivet och tillhörande nationell införlivandelagstiftning.

---

33 Se http://www.ecp.nl/projecten.php#32.

34 Enligt vissa av dessa villkor är man skyldig att med alla medel förhindra otillbörlig användning av tjänsterna i fråga. Andra villkor innehåller en hänvisning till befintliga yrkesetiska regler för masspost eller till självregleringsprinciper (t.ex. nätvett).

Inom ramen för kundtjänster måste man mer aktivt slå ett slag för filter genom att informera om skräppostfilter och genom att ge användarna möjlighet att välja filtertjänster eller filterfunktioner.

Samma sak gäller när Internetleverantörer eller mobiloperatörer sluter avtal med tredje part, i synnerhet när det gäller reklambyråer som använder direkt marknadsföring. Detta gäller inte bara direkta relationer med tjänsteföretag. Det gäller också de operatörer med vilka en tjänsteleverantör har slutit samtrafiksavtal, t.ex. i samband med mobila tjänster.

Det nya opt-in-systemet påverkar också flera områden för direkt marknadsföring, exempelvis

- metoderna för insamling av e-postadresser och andra elektroniska kontaktuppgifter (såsom nämnts ovan är okontrollerad insamling av e-postadresser inte förenlig med gemenskapslagstiftningen),

- anpassningen av befintliga listor,

- förbudet mot användning av uppgifter utan samtycke och mot försäljning av olagliga listor.

4.1.2. Föreslagna åtgärder

Medverkan från näringslivet och självreglering, eller ännu hellre samreglering, bör främjas, särskilt på områden där det eventuellt inte räcker med lagstiftning och myndigheternas verkställande av gällande regler. Alla berörda parter bör dra sitt strå till stacken, även konsument- och användarorganisationer.

Tjänsteleverantörernas avtalsvillkor gentemot abonnenter och affärspartner

Näringslivet måste först och främst undersöka om deras befintliga avtal är förenliga med de nya reglerna och anpassa dem vid behov.

Detta gäller anpassningen av abonnenternas avtalsvillkor. Inte bara Internet- och e-postleverantörer berörs av detta utan också leverantörer av mobila tjänster. Utöver detta skulle man inom ramen för sina kundtjänster som tillval kunna tillhandahålla information om filter och om filterprogram eller filtertjänster (se avsnitt 4.3). Även bestämmelserna i avtal med affärspartner (t.ex. mobil samtrafik och mervärdestjänster) bör vara utformade så att marknadsföringsmetoderna är förenliga med opt-in-principen och att eventuella överträdelser är förenade med lämpliga påföljder.

Masspostarnas metoder

För det andra måste reklambyråer som använder direkt marknadsföring, dvs. masspostare, eventuellt anpassa sina metoder till opt-in-systemet. Masspostarna skulle bland annat kunna enas om särskilda lagenliga metoder för insamling av personuppgifter (t.ex. dubbel eller bekräftad opt-in).

Yrkesetiska regler

För det tredje har olika branschorganisationer redan meddelat en rad initiativ, exempelvis antagandet av yrkesetiska regler och spridning av god marknadsföringssed[35]. Kommissionen ställer sig bakom idén med nätbaserade europatäckande yrkesetiska regler för direkt marknadsföring. Alla yrkesetiska regler och alla andra självregleringsinitiativ och avtal måste följa opt-in-reglerna. I detta hänseende kan medverkan från den behöriga tillsynsmyndigheten vara värdefull. Det bör mot denna bakgrund påminnas om att artikel 29-arbetsgruppen för uppgiftsskydd kan godkänna EU-täckande yrkesetiska regler (se artikel 30 i det allmänna uppgiftsskyddsdirektivet 95/46/EG).

Ofta fungerar självregleringslösningar bara om det finns en struktur för övervakning av att de överenskomna reglerna följs, inklusive effektiva sanktioner.

Märkning

För att öka medvetenheten bland användarna kan man för det fjärde använda hjälpmedel såsom synlig märkning (kvalitetsmärkning), särskilt i de fall där en betrodd tredje part övervakar och intygar att marknadsaktörerna följer de yrkesetiska reglerna.

Synlig märkning hjälper användarna att se vilka Internetleverantörer, e-postleverantörer och andra branschaktörer som följer EU:s regler eller sådana yrkesetiska regler som bygger på dessa. Märkningen skulle också kunna göra filtersystemen mer effektiva.

Man skulle också kunna märka de användardatabaser och e-postmeddelanden som bygger på opt-in (t.ex. genom att skriva ”ADV” i rubriken på meddelanden med reklam).

Genom en sådan märkning blir det kommersiella meddelandet också klart identifierbart som sådant för mottagaren i enlighet med direktivet om elektronisk handel (se artikel 6 a i direktiv 2000/31/EG, se även avsnitt 2 ovan).

4.2. Mekanismer för alternativ tvistlösning

4.2.1. Bakgrund

När det gäller kränkning av integriteten genom exempelvis icke begärd e-post, kan en utomrättslig prövning bidra till en bättre efterlevnad av de nya reglerna. Både på nationell nivå och EU-nivå har det tagits olika initiativ till alternativ lösning av tvister i fråga om transaktioner och kommunikationer på nätet. Kommissionen antog 1998 och 2001 rekommendationer om alternativ tvistlösning och formulerade principerna för ett sådant system. Flera initiativ är på gång när det gäller konsumentskyddsrelaterade system för alternativ tvistlösning (t.ex. EEJ-NET)[36]. I artikel 17 i direktivet om elektronisk handel uppmuntras utvecklingen av sådana mekanismer.

Utomrättsliga förfaranden finns redan i en rad länder, ibland i lagstadgad form, men de skiljer sig åt i flera avseenden, bland annat i fråga om tillämpningsområde (exempelvis

---

35 Europeiska federationen för direkt marknadsföring (FEDMA) har meddelat att den på nätet tänker lägga ut särskilda yrkesetiska

36 Mer information finns på http://europa.eu.int/comm/consumers/redress/out_of_court/index_en.htm

branschspecifikt för direkt marknadsföring och e-postreklam), ”behörighet”, befogenheter och sanktioner (exempelvis skadestånd) och myndighetsmedverkan (exempelvis dataskyddsmyndigheter och organ för reklamnormer).

För att mekanismerna skall vara tillräckligt effektiva måste vissa förutsättningar vara uppfyllda, exempelvis i fråga om organisation, stöd för verksamheten och beslutens genomdrivande. För införandet av sådana mekanismer krävs också att myndigheter och näringsliv samarbetar.

4.2.2. Föreslagna åtgärder

Framtagande och användning av effektiva självreglerande klagomålsmekanismer och mekanismer för alternativ tvistlösning uppmuntras. De bör i möjligaste mån bygga på befintliga initiativ (t.ex. EEJ-NET). Särskilt när det är svårt att få till stånd ett internationellt samarbete kan sådana förfaranden vara till stor nytta.

4.3. Tekniska frågor

4.3.1. Bakgrund

På den tekniska fronten tillämpas olika lösningar i kampen mot skräppost. Internetorganen (t.ex. RIPE och IETF) ser allvarligt på skräppostproblemet[37]. Initiativ som gäller ett längre tidsperspektiv, t.ex. nya tekniska standarder för e-post, omfattas inte av detta dokument. Internet- och e-postleverantörer blockerar ofta inkommande e-postmeddelanden från servrar som används för att skicka ut skräppost (svartlistning) tills skräppostens avsändare har identifierats och hindrats från att använda servern. Dessutom kan den enskilda användaren, på sin terminalutrustning, eller e-postleverantören, på sin server, använda filterprogram.

Emellertid ger inte alla filtermetoder och filterlösningar användaren samma slags kontroll. De ger inte heller samma säkerhet när det gäller uppgiftsskydd och integritet, exempelvis konfidentialiteten vid kommunikation. Eventuellt är de heller inte anpassade till det nya opt-in-system som gäller för marknadsföringskommunikation i EU-länderna (samtyckesbaserad masspost och annan e-post för marknadsföring). Genom en bättre differentiering mellan legitim reklam (t.ex. reklam som bygger på opt-in) och skräppost är det eventuellt också möjligt att utveckla effektivare filter.

Visserligen ger de nya bestämmelserna om skräppost användaren bättre skydd och e-postleverantören större säkerhet, när de på begäran vidtar åtgärder mot skräppostare, men filtret kan ibland också sålla bort legitim e-post (så kallade falska positiva resultat) eller släppa igenom skräppost (falska negativa resultat). I vissa fall kan det därför finnas risk att en avsändare eller en tilltänkt mottagare vidtar rättsliga åtgärder mot Internet- eller e-postleverantören. En rad Internet- och e-postleverantörer erbjuder därför sina användare filtret som tillval och kräver att användaren ger sitt tillstånd innan filtret aktiveras.

---

[37] RIPE:s (*Réseaux IP Européens*) arbetsgrupp för bekämpning av skräppost har exempelvis varit aktiv sedan 1998 [se dokumentet *Good Practice for combating Unsolicited Bulk Email* (”god praxis i kampen mot icke begärd masspost”), som återfinns på RIPE:s webbplats http://www.ripe.net]. Nyligen inrättade IRTF (*Internet Research Task Force*) en forskningsgrupp för bekämpning av skräppost (se http://www.irtf.org/charters/asrg.html). Gruppen kommer eventuellt att ta fram vissa tekniska lösningar som utgångspunkt för standardiseringsarbetet inom IETF (*Internet Engineering Task Force*).

Filtertekniken mot skräppost leder också till andra frågor, som dock ligger utanför ramen för detta meddelande, exempelvis frågan om filter kontra yttrandefrihet eller filter kontra Internet- och e-postleverantörers avtalsenliga skyldighet att vidarebefordra sina kunders e-postmeddelanden.

Eftersom det för mobila tjänster används andra affärsmodeller än för fasta Internettjänster, krävs det för mobila tjänster eventuellt andra filterlösningar. Den viktigaste skillnaden är att det inom ramen för mobila tjänster krävs en avgift för varje meddelande, vilket gör skräppost mer kostsamt. Vissa nya tjänster innebär dock att avgiften tas ut vid mottagandet, vilket gör att skräpposten ökar mottagarens kostnader. Dessutom kan e-post numera också levereras till mobila terminaler. För att hjälpa de drabbade abonnenterna att få bukt med skräpposten skulle man kunna erbjuda dem filter och förtittsmöjligheter.

Uppmärksamhet bör också ägnas åt öppna reläer. Öppna reläer är SMTP-servrar som kan användas för vidarebefordran av e-post från avsändare som inte är lokala användare på servern. Tidigare var de flesta reläer öppna, men sådana reläer kan relativt enkelt utnyttjas av skräppostare. Genom enkla förebyggande åtgärder kan man minska möjligheterna för sådant missbruk. Samma sak gäller för öppna mellanservrar, dvs. servrar som via sina program är direktkopplade till Internet.

4.3.2. Föreslagna åtgärder

Medlemsstaterna och de behöriga myndigheterna uppmanas klargöra de rättsliga villkoren för användandet av olika filter i det egna landet, inklusive krav på integritetsskydd.

Filterleverantörer måste se till att deras system är förenliga med opt-in-systemet och andra krav i EU:s lagstiftning, inte minst kraven på konfidentialitet vid kommunikation.

Användarna bör ges möjlighet att själva bestämma hur den inkommande skräpposten skall hanteras. Filterleverantörer bör tänka på vilka följder falska positiva och falska negativa resultat, och vissa former av innehållsbaserad filtrering, kan få för användarna och vilka ansvarsfrågor detta kan leda till.

Filterleverantörer bör i samarbete med de berörda parterna utveckla filter som känner igen sådan e-postreklam som uppfyller gemenskapslagstiftningens krav när det gäller godkända marknadsföringsmetoder, inklusive kvalitetsmärkning och liknande.

E-postleverantörer (och i förekommande fall leverantörer av mobila tjänster) bör som tillval erbjuda sina kunder filtertjänster eller filterfunktioner och information om de filtertjänster och filterprodukter som slutanvändaren kan få av tredje part.

E-postservrarnas ägare bör se till att deras servrar är vederbörligen skyddade och inte kan användas som öppna reläer (utom i motiverade fall). Samma sak gäller för öppna mellanservrar.

5. ÅTGÄRDER FÖR ÖKAD MEDVETENHET

Detta avsnitt handlar om ökad medvetenhet och gäller bland annat förebyggande åtgärder, ökad konsumentmedvetenhet och rapportering.

5.1. Bakgrund

Medlemsstaterna skulle senast den 31 oktober 2003 ha införlivat det nya opt-in-systemet för icke begärd e-post med sin nationella lagstiftning. Det nya systemet har visserligen fått relativt stor uppmärksamhet i pressen, men bland marknadsaktörer och medborgare råder fortfarande osäkerhet om vad opt-in egentligen innebär i praktiken[38].

Det nya systemet bygger på att användaren själv skall kunna bestämma om han eller hon vill ha kommersiell kommunikation eller inte. För detta måste användaren dock veta vilka grundläggande regler som gäller för icke begärd kommunikation och vem man anmäler problem till.

Lyckade exempel

Den brittiska dataskyddsmyndigheten (Information Commissioner) offentliggjorde några veckor före ikraftträdandet av de nya bestämmelser som antagits för att genomföra direktivet en vägledning om de nya brittiska reglerna, där ett särskilt avsnitt ägnas åt reklam med elektroniska medel. Vidare meddelades att blanketter för klagomål skulle läggas ut på nätet och finnas tillgängliga i dataskyddsmyndighetens lokaler med nödvändiga närmare uppgifter, när reglerna väl trätt i kraft[39].

Användarna måste också vara medvetna om de risker som är förknippade med utlämnandet av personuppgifter på Internet (t.ex. på webbsidor eller i diskussionsgrupper) och anpassa sitt beteende därefter.

Sist men inte minst bör de veta vilka filter som finns på marknaden och vad tjänste- och programleverantörer (t.ex. Internet- och e-postleverantörer) kan göra för dem.

Lyckade exempel

Den franska dataskyddsmyndigheten CNIL har på sin webbplats lagt ut omfattande information om skräppostrelaterade frågor, bland annat om erfarenheterna av e-postlådan för skräppostklagomål, fall som anmälts till de rättsliga myndigheterna (se nedan), grundläggande tips för hur man kan förebygga skräppost, information om vem man kan anmäla skräppost till och hänvisningar till relevanta användarorganisationer.

Åtgärder för att informera om det nya opt-in-systemet har visserligen vidtagits eller planeras i de flesta medlemsstater, men det råder stora skillnader i fråga om tidpunkt, innehåll, målgrupp och medverkande parter. Några medlemsstater väntar tills lagarna har antagits. Efter varje offentligt samråd om genomförandet av direktiv 2002/58/EG har medvetenheten ökat något.

Beroende på befogenheterna är olika myndigheter ansvariga för dessa insatser i medlemsstaterna (exempelvis dataskyddsmyndigheter, tillsynsmyndigheter, konsumentskyddsmyndigheter eller ombudsmän). De olika behöriga myndigheternas verksamheter samordnas (ännu) inte i alla medlemsstater. Till dem som är inblandade hör

---

38 Bakgrundsinformation om reglerna för icke begärd kommunikation enligt direktiv 2002/58/EG återfinns på följande webbadress: http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited

39 Se http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_2002/58/EC.html#guidance

ofta branschorganisationer, konsument- och användarorganisationer och ibland till och med ministerier.

Även vissa sektorer inom näringslivet har gjort insatser för att öka medvetenheten på nationell, europeisk eller global nivå, och även här är skillnaderna stora. Till exempel:

– Praktiska vägledningar för masspostare eller informationskampanjer med särskild inriktning på kommunikationssektorn.
– Allmän vägledning för kunderna om yrkesetiska regler, klagomålsmekanismer och filter.
– Plattformar/arbetsgrupper för framtagande av god sed för kommersiell kommunikation.

5.2. Föreslagna åtgärder

För att det verkligen skall bli klart vad som är rätt och fel när det gäller kommersiell e-post krävs det på kort sikt omfattande och ihållande insatser i samtliga medlemsstater både när det gäller förebyggande och rättsliga åtgärder. Det bör finnas praktisk information om förebyggande åtgärder, godtagbara marknadsföringsmetoder samt tekniska och rättsliga lösningar för användaren.

Alla parter uppmanas medverka i de åtgärder som vidtas för att öka medvetenheten, både medlemsstater och behöriga myndigheter, liksom företag och konsument- och användarorganisationer. Där så ännu inte har skett uppmanas medlemsstater och behöriga myndigheter att inleda eller främja informationskampanjer i början av 2004.

När det gäller innehåll bör de åtgärder som är inriktade på företag och/eller konsumenter omfatta följande:

– En grundläggande men allmänt spridd förståelse av de nya reglerna och rättigheterna.

– Praktisk information om godtagbara marknadsföringsmetoder inom ramen för opt-in-systemet, inklusive klargörande om legitim insamling av personuppgifter.

– Praktisk information för konsumenter om hur man undviker skräppost (t.ex. om utlämnande av personuppgifter).

Skräppost och handlingsplanen för ett säkrare Internet

Kommissionen har inom ramen för handlingsprogrammet för ett säkrare Internet offentliggjort en ansökningsomgång för att få förslag till projekt mot skräppost på olika områden, t.ex. ökad medvetenhet. Projekt som väljs ut vid ansökningsomgångens första utvärdering skulle kunna inledas i maj 2004.

Kommissionen är i färd med att utarbeta ett förslag till ett uppföljningsprogram, *Safer Internet plus*, för att finansiera ytterligare åtgärder mot olagligt och skadligt innehåll samt oönskat innehåll såsom skräppost.

http://www.europa.eu.int/information_society/programmes/iap/call/index_en.htm

– Praktisk information för konsumenter om de produkter och tjänster som kan användas för att undvika skräppost (t.ex. filter och säkerhetsfunktioner).
– Information om vad man kan göra om man drabbas av skräppost, bland annat information om klagomålsmekanismer och, i förekommande fall, system för alternativ tvistlösning.

Målgrupper för åtgärderna är

a) företag som medverkar i eller använder direkt marknadsföring,
b) konsumenter som abonnerar på e-posttjänster, inklusive SMS-tjänster, och
c) e-postleverantörer och leverantörer av mobila tjänster.

Informationen bör spridas genom flera olika kanaler (inte bara på nätet), så att man verkligen når alla målgrupper. Det är därför viktigt att även få näringslivet och konsumentorganisationer att medverka. De olika initiativen bör samordnas.

De ovannämnda åtgärderna bör också handla om effektiva yrkesetiska regler, klagomålsmekanismer, kvalitetsmärkning och, i förekommande fall, system för certifiering.

Kommissionen tillhandahåller redan grundläggande information om opt-in-systemet på Europa-webbplatsen[40]. Där kommer det också att finnas länkar med information om nationella genomförandefrågor och, i den mån uppgifterna finns tillgängliga, siffror och trender i fråga om skräppost. Kommissionen kommer också att utnyttja euroinfocentrena för att sprida information om de nya reglerna.

SLUTSATS

Skräppost är i dag ett av de största problemen på Internet. Åtgärder mot skräppost måste vidtas på flera olika fronter och, vid sidan om ett effektivt verkställande av reglerna och internationellt samarbete, också inriktas på tekniska lösningar och självreglering inom näringslivet samt ökad konsumentmedvetenhet. De åtgärder som presenteras i detta meddelande sammanfattas i nedanstående tabell.

Kommissionen kommer visserligen att stödja dessa ansträngningar i möjligaste mån, men det är i första hand EU:s medlemsstater, behöriga myndigheter, näringsliv, konsumenter, Internetanvändare och användare av elektroniska kommunikationstjänster som måste ta sitt ansvar, både på nationell och på internationell nivå.

Genom att parallellt och på ett integrerat sätt genomföra de olika åtgärder som presenteras i detta meddelande, och som får brett stöd av berörda parter, kan man bidra till att avsevärt minska mängden av den skräppost som för närvarande äventyrar e-postens och annan elektronisk kommunikations fördelar för samhället och ekonomin.

Kommissionen kommer att övervaka åtgärdernas genomförande under 2004, bland annat med hjälp av den informella skräppostgruppen. Kommissionen kommer senast i slutet av 2004 att undersöka om det behövs ytterligare eller korrigerande åtgärder.

[40] http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm

TABELL MED DE ÅTGÄRDER SOM PRESENTERAS I MEDDELANDET

I nedanstående tabell sammanfattas de åtgärder som presenteras i meddelandet. Kommissionens åtgärder är uppförda för sig. Såsom redan nämnts är åtgärderna kopplade till varandra på olika sätt och bör i möjligaste mån genomföras parallellt och på ett integrerat sätt.

I – Effektivt genomförande och verkställande i medlemsstaterna och genom behöriga myndigheter

Först och främst bör medlemsstaterna omgående införliva direktivet om integritet och elektronisk kommunikation med sin lagstiftning, i synnerhet bestämmelserna om icke begärd kommunikation.

Medlemsstaterna och de behöriga myndigheterna bör undersöka hur effektiva deras verkställighetsmekanismer är i fråga om korrigerande åtgärder och påföljder, klagomålsmekanismer, EU-samarbete, samarbete med tredje land och övervakning. Medlemsstaterna bör också ta fram nationella strategier för att få dataskyddsmyndigheter, konsumentskyddsmyndigheter och nationella tillsynsmyndigheter att samarbeta så att man undviker dubbelarbete och överlappning av verksamheter.

Medlemsstaternas och de behöriga myndigheternas viktigaste åtgärder:

a) Effektiva korrigerande åtgärder och påföljder

- Att se till att de drabbade kan kräva rimligt skadestånd och att det finns kännbara sanktioner, vid behov även ekonomiska och straffrättsliga sanktioner.

- Att överväga införandet av administrativa förfaranden för att se till att de nya reglerna följs i de medlemsstater där sådana förfaranden ännu saknas.

- Att ge de behöriga myndigheterna den behörighet som krävs för undersökningar och ingripanden.

b) Klagomålsmekanismer

- Att införa lämpliga klagomålsmekanismer, bland annat en särskild e-postlåda för användarklagomål.

- Att samordna de berörda nationella myndigheternas åtgärder.

c) Gränsöverskridande klagomål och verkställighetssamarbete inom EU

- Att tillämpa en befintlig, eller vid behov nyskapad, samordningsmekanism för samarbete mellan de nationella tillsynsmyndigheterna när det gäller verkställande av lagar över gränserna (informationsutbyte, ömsesidigt bistånd) inom EU. Rådet och parlamentet uppmanas mot denna bakgrund, och särskilt när det gäller bedräglig och försåtlig skräppost, att så snart som möjligt enas om den föreslagna förordningen om konsumentskyddssamarbete och att undersöka huruvida förordningen även skall omfatta direktivet om integritet och elektronisk kommunikation.

d) Samarbete med tredje land

- Att aktivt medverka i multilaterala fora (exempelvis OECD) för att hitta lösningar på internationell nivå.

- Att stärka respektive inleda bilateralt samarbete med tredje land.

- Att tillsammans med kommissionen undersöka vilka initiativ som kan tas för att förbättra det internationella samarbetet.

- Att samarbeta med den privata sektorn när det gäller att spåra skräppostare, förutsatt att det finns lämpliga rättsliga garantier.

e) Övervakning

- Att se till att de får den information och de statistiska uppgifter de behöver för att se till att reglerna följs, i förekommande fall i samarbete med näringslivet och med hänsyn till OECD:s pågående mätningar.

II – Självreglering och tekniska åtgärder inom näringslivet

Marknadsaktörerna (exempelvis Internet- och e-postleverantörer, mobiloperatörer, programföretag och masspostare) bör sträva efter att göra opt-in-systemet till normal praxis, i samarbete med konsument- och användarorganisationer och behöriga myndigheter. Åtgärderna bör bland annat inriktas på följande:

a) Självreglering

- Att utvärdera, och vid behov anpassa, tjänsteleverantörernas (Internet- och e-postleverantörer, mobiloperatörer) avtalsvillkor gentemot abonnenter och företagspartner, och att informera kunderna om filter och eventuellt att som tillval erbjuda dem filterprogram eller filtertjänster.

- Att anpassa metoderna för direkt marknadsföring till opt-in-systemet, och att eventuellt enas om särskilda lagenliga metoder för insamling av personuppgifter (t.ex. dubbel eller bekräftad opt-in).

- Att utarbeta och sprida effektiva yrkesetiska regler (t.ex. FEDMA-initiativet), som är förenliga med opt-in-systemet, där så är lämpligt i samarbete med artikel 29-arbetsgruppen för uppgiftsskydd eller behöriga nationella myndigheter.

- Att överväga en märkning av de e-postmeddelanden och databaser som bygger på opt-in så att användarna (och filtren) lättare kan känna igen dem som sådana, i enlighet med direktivet om elektronisk handel.

- Att använda, eller vid behov ta fram, effektiva självreglerande klagomålsmekanismer och mekanismer för alternativ tvistlösning, som i möjligaste mån bygger på befintliga initiativ (t.ex. EEJ-NET).

b) Klagomålsmekanismer

- (Filterleverantörer) Att se till att deras system är förenliga med opt-in-systemet och andra krav i EU:s lagstiftning, inte minst kraven på konfidentialitet vid kommunikation. Medlemsstaterna och de behöriga myndigheterna uppmanas klargöra de rättsliga villkoren för användandet av olika filter i det egna landet, inklusive krav på integritetsskydd.

- (Filterleverantörer) Att tänka på vilka följder falska positiva och falska negativa resultat, och vissa former av innehållsbaserad filtrering, kan få för användarna och vilka ansvarsfrågor detta kan leda till. Användarna bör ges möjlighet att själva bestämma hur den inkommande skräpposten skall hanteras.

- (Filterleverantörer) Att i samarbete med de berörda parterna utveckla filter som känner igen legitim e-postreklam (dvs. reklam som uppfyller gemenskapslagstiftningens krav när det gäller godkända marknadsföringsmetoder), exempelvis kvalitetsmärkta meddelanden.

- (E-postleverantörer och i förekommande fall leverantörer av mobila tjänster) Att som tillval erbjuda sina kunder filtertjänster eller filterfunktioner och information om de filtertjänster och filterprodukter som slutanvändaren kan få av tredje part.

- (E-postservrarnas ägare) Att se till att deras servrar är vederbörligen skyddade och inte kan användas som öppna reläer (utom i motiverade fall). Samma sak gäller för öppna mellanservrar.

III – Åtgärder för ökad medvetenhet att vidtas av medlemsstater, näringslivet och konsument- och användarorganisationer

Där så ännu inte har skett uppmanas medlemsstater och behöriga myndigheter att inleda eller främja informationskampanjer i början av 2004.

Alla parter, medlemsstater, behöriga myndigheter, företag och konsument- och användarorganisationer, bör aktivt tillhandahålla praktisk information om förebyggande åtgärder, godtagbara marknadsföringsmetoder samt tekniska och rättsliga lösningar för användarna, och bland annat göra följande:

- Inrikta åtgärderna på a) företag som medverkar i eller använder direkt marknadsföring, b) konsumenter som abonnerar på e-posttjänster, inklusive SMS-tjänster, och c) e-postleverantörer och leverantörer av mobila tjänster.

- Se till att företag och/eller konsumenter får

- en grundläggande men allmänt spridd förståelse av de nya reglerna och rättigheterna,

- praktisk information om godtagbara marknadsföringsmetoder inom ramen för opt-in-systemet, inklusive klargörande om legitim insamling av personuppgifter,

- praktisk information för konsumenter om hur man undviker skräppost (t.ex. utlämnande av personuppgifter),

- praktisk information för konsumenter om de produkter och tjänster som kan användas för att undvika skräppost (t.ex. filter och säkerhetsfunktioner),

- information om vad man kan göra om man drabbas av skräppost, bland annat information om klagomålsmekanismer och, i förekommande fall, system för alternativ tvistlösning.

- Hänvisa till effektiva yrkesetiska regler, klagomålsmekanismer, kvalitetsmärkning och, i förekommande fall, system för certifiering.

- Sprida informationen genom flera olika kanaler, via nätet och på andra vägar, så att man verkligen når alla målgrupper.

Det är därför viktigt att även få näringslivet och konsumentorganisationer att medverka. De olika initiativen bör samordnas.

IV – Åtgärder att vidtas av kommissionen

Kommissionen kommer att övervaka ovannämnda åtgärders genomförande under 2004, bland annat med hjälp av den informella skräppostgruppen, och kommer senast i slutet av 2004 att undersöka om det behövs ytterligare eller korrigerande åtgärder.

Kommissionen kommer även fortsättningsvis att noga följa direktivets genomförande. Kommissionen kommer bland annat att förvissa sig om att de nationella genomförandeåtgärderna leder till kännbara sanktioner, vid behov även ekonomiska och straffrättsliga, om de relevanta kraven inte uppfylls. (Kommissionen inledde i november 2003 överträdelseförfaranden mot en rad medlemsstater som inte hade anmält några genomförandeåtgärder.) Vid behov är kommissionen beredd att bistå medlemsstaterna i detta.

Kommissionen har, med medlemsstaternas och dataskyddsmyndigheternas stöd, tillsatt en informell och nätbaserad skräppostgrupp. Gruppen kommer att underlätta genomförandet av verkställighetsåtgärder (t.ex. klagomål, korrigerande åtgärder, påföljder och internationellt samarbete) och andra åtgärder som presenteras i detta meddelande.

Kommissionen kommer att uppmana artikel 29-arbetsgruppen för uppgiftsskydd att så snart som möjligt yttra sig om några av de lösningar som beskrivs i direktivet om integritet och elektronisk kommunikation för att bidra till en enhetlig tillämpning av nationella åtgärder enligt direktivet.

Kommissionen har i samarbete med medlemsstaterna och nationella verkställighetsmyndigheter börjat undersöka hur man bäst sörjer för verkställande av lagar över gränserna inom och utanför EU. Arbetet med de nationella myndigheterna kommer att fortsätta under hela 2004.

Kommissionen ställer sig bakom idén med nätbaserade europatäckande yrkesetiska regler för direkt marknadsföring och stöder i förekommande fall att de godkänns av artikel 29-arbetsgruppen för uppgiftsskydd.

Kommissionen kommer att arrangera en OECD-workshop om skräppost i februari 2004 och kommer att diskutera uppföljningsåtgärder med medlemsstaterna, bland annat arbete inom OECD för att främja effektiv lagstiftning på internationell nivå, ökad medvetenhet, tekniska lösningar, självreglering och internationellt samarbete för att se till att reglerna följs.

Kommissionen kommer också att undersöka hur man bäst kan följa upp resultaten från 2003 års världstoppmöte om informationssamhället i EU, med hänsyn tagen till toppmötet i Tunis 2005.

Kommissionen har inom ramen för handlingsprogrammet för ett säkrare Internet offentliggjort en ansökningsomgång för att få förslag till projekt mot skräppost på olika områden. Kommissionen är i färd med att utarbeta ett förslag till ett uppföljningsprogramprogram, Safer Internet plus, för att finansiera ytterligare åtgärder mot bland annat skräppost.

Kommissionen kommer att fortsätta att tillhandahålla grundläggande information om opt-in-systemet på Europa-webbplatsen.

Där kommer det också att finnas länkar med information om nationella genomförandefrågor och, i den mån uppgifterna finns tillgängliga, siffror och trender i fråga om skräppost. Kommissionen kommer också att utnyttja euroinfocentrerna för att sprida information om de nya reglerna.