



**CONSIGLIO  
DELL'UNIONE EUROPEA**

**Bruxelles, 27 gennaio 2004 (19.02)  
(OR. fr)**

**5691/04**

**TELECOM 11**

**NOTA DI TRASMISSIONE**

---

Origine: Signora Patricia BUGNOT, Direttore, per conto del Segretario Generale della Commissione europea  
Data di ricezione: 23 gennaio 2004  
Destinatario: Signor Javier SOLANA, Segretario Generale/Alto Rappresentante  
Oggetto: Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa alle comunicazioni commerciali indesiderate (spam)

---

Si trasmette in allegato, per le delegazioni, il documento della Commissione COM(2004) 28 defin..

All.: COM(2004) 28 defin.



COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 22.01.2004  
COM(2004) 28 definitivo

**COMUNICAZIONE DELLA COMMISSIONE  
AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO SOCIALE ED  
ECONOMICO EUROPEO E AL COMITATO DELLE REGIONI**

**relativa alle comunicazioni commerciali indesiderate (spam)**

## INDICE

Sintesi .....	4
Contesto e finalità.....	5
1. Il problema dello Spam .....	7
1.1. Le dimensioni del problema.....	7
1.2. Perché lo spam è un problema?.....	8
2. Sintesi delle norme che disciplinano le comunicazioni commerciali indesiderate .....	9
2.1. Regime del consenso preliminare (“opt-in”).....	9
2.2. Disposizioni esecutive.....	11
2.3. Altre disposizioni applicabili in materia di spam.....	12
3. Attuazione ed applicazione efficaci da parte degli Stati membri e delle pubbliche autorità.....	13
3.1. Introduzione .....	14
3.2. Ricorsi e sanzioni efficaci .....	16
3.2.1. Discussione.....	16
3.2.2. Azioni proposte .....	17
3.3. Meccanismi di reclamo .....	17
3.3.1. Discussione.....	17
3.3.2. Azioni proposte .....	18
3.4. Reclami transfrontalieri e cooperazione in materia di controllo dell’applicazione all'interno dell'UE.....	19
3.4.1. Discussione.....	19
3.4.2. Azioni proposte .....	19
3.5. Cooperazione con i paesi terzi .....	20
3.5.1. Discussione.....	20
3.5.2. Azioni proposte .....	21
3.6. Monitoraggio .....	22
3.6.1. Discussione.....	22
3.6.2. Azioni proposte .....	22
4. Azioni tecniche e azioni di autoregolamentazione da parte dell’industria .....	23

4.1.	Applicazione efficace del regime “opt-in” .....	23
4.1.1.	Discussione.....	23
4.1.2.	Azioni proposte .....	24
4.2.	Meccanismi alternativi di composizione delle controversie .....	25
4.2.1.	Discussione.....	25
4.2.2.	Azioni proposte .....	26
4.3.	Questioni tecniche .....	26
4.3.1.	Discussione.....	26
4.3.2.	Azioni proposte .....	27
5.	Azioni di sensibilizzazione.....	28
5.1.	Discussione.....	28
5.2.	Azioni proposte .....	29
	Conclusioni.....	31
	Tabella delle azioni individuate nella comunicazione.....	32

**COMUNICAZIONE DELLA COMMISSIONE  
AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO SOCIALE  
ED ECONOMICO EUROPEO E AL COMITATO DELLE REGIONI**

**relativa alle comunicazioni commerciali indesiderate (spam)**

(Testo rilevante ai fini del SEE)

**SINTESI**

Le comunicazioni commerciali indesiderate inviate per posta elettronica, fenomeno conosciuto anche come “spam”, hanno raggiunto proporzioni preoccupanti. Si stima infatti che oltre il 50% del traffico mondiale di posta elettronica sia costituito da spam. Ancor più preoccupante è il tasso di crescita del fenomeno: nel 2001 la percentuale degli spam era appena del 7%.

Lo spam rappresenta un problema sotto diversi aspetti: violazione della privacy, abuso dei consumatori, protezione dei minori e della dignità umana, costi supplementari per le imprese, calo della produttività. In termini più generali lo spam intacca la fiducia dei consumatori che è una condizione indispensabile per il successo del commercio elettronico, dei servizi elettronici e di conseguenza per l'intera società dell'informazione.

L'UE ha previsto questo rischio adottando, nel luglio 2002, la direttiva 2002/58/CE sulla tutela della vita privata e le comunicazioni elettroniche, grazie alla quale è stato introdotto il principio di “opt-in”, ossia di consenso preliminare obbligatorio del destinatario del messaggio di posta elettronica (ma anche di SMS o MMS), oltre ad altre misure di tutela dei consumatori. Il termine ultimo di attuazione della direttiva era il 31 ottobre 2003. Procedimenti di infrazione sono stati avviati nei confronti di diversi Stati membri per mancata notifica alla Commissione dei provvedimenti attuativi nel diritto interno.

L'adozione della legislazione rappresenta il primo passo necessario, ma costituisce solo parte della soluzione al problema. La presente comunicazione individua una serie di interventi necessari ad integrazione delle norme adottate dall'UE in modo da fare del divieto di spam una realtà effettiva.

Non esistono formule magiche contro lo spam; le azioni elencate nella presente comunicazione si incentrano soprattutto sull'applicazione delle norme esistenti da parte degli Stati membri e delle pubbliche autorità, su soluzioni tecniche e di autoregolamentazione adottate dall'industria e infine sulla sensibilizzazione dei consumatori. Viene evidenziata anche la dimensione internazionale della problematica in quanto gran parte dello spam è generato al di fuori dell'Unione europea.

Queste azioni rispecchiano ampiamente il consenso emerso nel corso del 2003 e confermato in occasione di un *workshop* pubblico tenutosi nell'ottobre 2003; sarà tuttavia altrettanto importante ottenere un consenso anche in merito alla loro attuazione. Solo grazie allo sforzo congiunto di tutti, dagli Stati membri alle pubbliche autorità, alle imprese, fino ai consumatori e agli utenti di Internet e delle comunicazioni elettroniche sarà possibile arginare il fenomeno dello spam.

Alcune di queste azioni comportano evidenti costi ma si tratta del prezzo da pagare per la sopravvivenza dell'e-mail e dei servizi elettronici in generale quali strumenti di comunicazione efficaci. La messa in atto delle azioni individuate nella presente comunicazione contribuirà in modo considerevole a ridurre il volume degli spam, nell'interesse della società dell'informazione, dei nostri cittadini e delle nostre economie.

### **Contesto e finalità**

Il fenomeno dei messaggi commerciali indesiderati inviati per posta elettronica<sup>1</sup>, detto "spam", è considerato ormai il principale problema a cui deve far fronte Internet. Il fenomeno ha infatti assunto proporzioni preoccupanti al punto che si corre il rischio che gli utenti cessino di utilizzare l'e-mail – una delle applicazioni Internet più diffuse – gli SMS e le altre applicazioni mobili o ne facciano un uso meno intensivo di quello che ne farebbero in assenza di spam. In linea generale, poiché Internet e gli altri mezzi di comunicazione elettronica (accesso a banda larga, accesso senza filo, comunicazioni mobili...) sono chiamati ad essere i fattori essenziali dell'aumento di produttività delle economie moderne, lo spam merita un'attenzione ancora maggiore.

Per quanto sia condivisa la necessità di un intervento prima che gli inconvenienti legati alla proliferazione dello spam non vanifichino i vantaggi che l'e-mail e gli altri servizi mobili recano alle aziende e ai cittadini, la scelta degli strumenti per contrastare il fenomeno non è semplice, tanto più che non esistono soluzioni magiche in questo campo. Solo l'azione congiunta di tutti gli attori interessati, dagli Stati membri alle autorità nazionali competenti, alle imprese, fino ai consumatori e agli utenti di Internet e delle comunicazioni elettroniche, permetterà di contrastare efficacemente questo fenomeno.

La presente comunicazione individua una serie di azioni di tipo giuridico, tecnico e di sensibilizzazione basate sulla direttiva 2002/58/CE, che stabilisce un sistema di consenso preliminare (detto "opt-in") e che gli Stati membri erano tenuti a mettere in atto entro il 31 ottobre 2003<sup>2</sup>.

Queste azioni si incentrano soprattutto su un'efficace attuazione e applicazione della direttiva da parte degli Stati membri, su misure tecniche, sull'autoregolamentazione da parte dell'industria, sulla sensibilizzazione dei consumatori e sulla cooperazione internazionale. La dimensione internazionale è indispensabile in questo campo in quanto gran parte dello spam ha origine al di fuori dell'Unione europea e in particolare in America del Nord<sup>3</sup>.

---

<sup>1</sup> La presente comunicazione non verte sulle comunicazioni indesiderate non effettuate per via elettronica (ad es. le comunicazioni postali).

<sup>2</sup> Cfr. in particolare l'articolo 13 della direttiva 2002/58/CE sulla protezione della vita privata nel settore delle comunicazioni elettroniche (cfr. capitolo 2).

<sup>3</sup> Ad esempio, le iniziative "boîte à spam" organizzate nel 2002 dalla *Commission Nationale Informatique et Libertés* – CNIL (Francia) e dalla *Commission de la Protection de la Vie Privée* – CPVP (Belgio) sembrano confermare che gli Stati Uniti e in minor misura il Canada sono le fonti principali di messaggi spam. I risultati dell'indagine effettuata dalla CPVP sono consultabili all'indirizzo: [http://www.privacy.fgov.be/publications/spam\\_4-7-03\\_fr.pdf](http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf) mentre la relazione della CNIL è consultabile all'indirizzo: [http://www.cnil.fr/thematic/docs/internet/boite\\_a\\_spam.pdf](http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf) Cfr. anche: UNCTAD, *E-Commerce and Development Report 2003*, New York e Ginevra, 2003, pag. 27.

Queste azioni rispecchiano ampiamente il consenso emerso nel corso del 2003 e confermato nel quadro di un *workshop* pubblico tenutosi nell'ottobre 2003<sup>4</sup>. Il consenso in questo settore è un elemento essenziale perché sono in primo luogo le parti interessate – con il sostegno, ove possibile, della Commissione – a dover dare attuazione alle azioni individuate, nell'interesse della società dell'informazione, dell'industria e degli utenti.

### **Struttura del documento**

Il presente documento individua una serie di aspetti specifici della problematica spam e propone azioni precise da attuare per ciascuno di tali aspetti. Le migliori pratiche vengono poste in evidenza ogniqualvolta necessario.

Le azioni proposte sono ordinate in base alla seguente struttura:

- **Azioni di attuazione e di applicazione** – Sono destinate principalmente ai governi e alle pubbliche autorità e comprendono ricorsi, sanzioni, meccanismi di reclamo (anche transfrontalieri), cooperazione con paesi terzi, monitoraggio (capitolo 3).
- **Azioni di autoregolamentazione e azioni tecniche** – Sono principalmente destinate agli operatori del mercato e vertono su disposizioni contrattuali, codici di condotta, pratiche commerciali accettabili, marchi, meccanismi alternativi di composizione delle controversie e soluzioni tecniche (filtraggio, sicurezza ...) (capitolo 4).
- **Azioni di sensibilizzazione** – Sono destinate ai governi e alle pubbliche autorità, agli operatori del mercato, alle associazioni di difesa dei consumatori e agli organismi analoghi e vertono sulla prevenzione, l'educazione dei consumatori e i meccanismi di segnalazione (capitolo 5).

**Le azioni suelencate sono riassunte in una tabella riportata alla fine della comunicazione.** Esse sono intercorrelate in diversi modi e devono essere attuate nella misura del possibile in modo parallelo ed integrato.

Prima di entrare nel merito delle azioni, i capitoli che seguono analizzano il fenomeno dello spam in quanto tale (capitolo 1) e richiamano le nuove norme applicabili dal 31 ottobre 2003 (capitolo 2).

---

<sup>4</sup> In preparazione del seminario è stato distribuito un documento di riflessione sulle comunicazioni indesiderate (o spam) elaborato sulla base delle discussioni precedentemente tenutesi nell'ambito del comitato COCOM e del gruppo di lavoro "Articolo 29 – protezione dati". I membri del comitato COCOM e del gruppo di lavoro "articolo 29" hanno fornito informazioni in risposta ad un questionario. Hanno inoltre reagito diverse associazioni settoriali e singole imprese (ISP, operatori di reti fisse e mobili, società di commercializzazione diretta, agenzie di pubblicità, fabbricanti di computer e fornitori di software).

## 1. IL PROBLEMA DELLO SPAM

### Cosa si intende per spam?

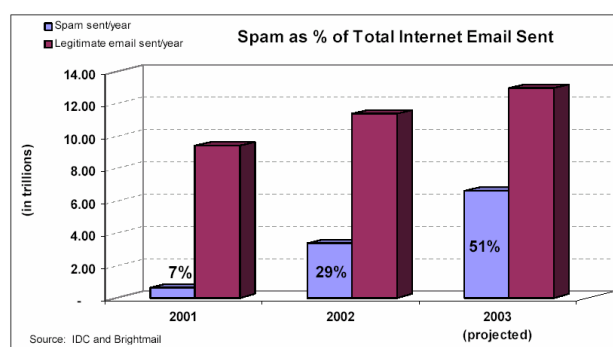
“Spam” è un termine spesso utilizzato ma raramente definito. Viene impiegato in genere per designare l’invio, spesso indiscriminato, di messaggi elettronici non richiesti. La nuova direttiva non definisce né utilizza il termine spam. Si rifà invece ai concetti di “comunicazioni indesiderate a scopo di commercializzazione diretta” inviate per “posta elettronica” che, presi congiuntamente, coprono la maggior parte delle fattispecie degli spam. La presente comunicazione utilizza pertanto spam come sinonimo conciso di “comunicazioni commerciale indesiderata inviata per posta elettronica”.

Si noti che lo stesso concetto di “posta elettronica” non designa solo i tradizionali messaggi elettronici basati sul protocollo SMTP, ma anche SMS, MMS e qualsiasi altra forma di comunicazione elettronica che non richiede la partecipazione simultanea del mittente e del destinatario (cfr. capitolo 2).

### 1.1. Le dimensioni del problema

I messaggi commerciali e-mail indesiderate – lo spam, quindi – hanno raggiunto proporzioni preoccupanti. Malgrado le variazioni nelle statistiche, si considera che oltre il 50% del traffico e-mail mondiale sia composto da spam.

Ancor più preoccupante è il tasso di crescita del fenomeno: nel 2001 la percentuale degli spam era ‘solo’ del 7%. Per il 2002, la percentuale degli spam è stimata al 29% mentre le proiezioni relative al 2003 indicano una percentuale del 51%.



**Figura 1: Proporzione degli spam rispetto al volume complessivo di e-mail inviate via Internet**

Possono esistere variazioni notevoli in funzione delle categorie di utenti e delle regioni del mondo. (Si stima ad esempio che il 30% delle e-mail che la Commissione europea riceve dall’esterno sia spam). In genere, tuttavia, i dati recenti relativi all’Unione europea sono altrettanto preoccupanti che quelli mondiali<sup>5</sup>.

Benché le comunicazioni indesiderate o lo spam rappresentino al momento un problema meno rilevante sulle reti mobili (ad esempio per i messaggi SMS), sviluppi tecnologici quali l’e-mail sui cellulari potrebbero portare ad un aumento del volume dello spam. L’esperienza dei paesi con una forte utenza dei servizi I-mode (come il Giappone) conferma del resto questa tendenza.

<sup>5</sup> Nel settembre 2003 si stima che la proporzione di spam nell’UE sia stata del 49%, rispetto ad una proporzione mondiale del 54% nello stesso periodo (fonte: Briggmail, 2003).

## 1.2. Perché lo spam è un problema?

Dal punto di vista del singolo individuo lo spam è un'intrusione nella vita privata. Questa preoccupazione è al centro delle nuove norme sulle comunicazioni indesiderate descritte nel capitolo seguente. Inoltre, lo spam è spesso ingannevole e fuorviante. Gran parte dello spam sembra mosso dalla volontà di imbrogliare i consumatori con menzogne e dichiarazioni fallaci<sup>6</sup>. Purtroppo troppi consumatori rispondono a questi messaggi ingannevoli e fuorvianti<sup>7</sup>. Anche i messaggi a carattere pornografico possono essere sconvolgenti<sup>8</sup>. La pulizia della mailbox richiede tempo e, se l'utente deve ricorrere a software di filtraggio e di altro tipo, anche denaro.

### Il pubblico è sensibile al fenomeno?

Il numero di reclami è rivelatore della preoccupazione degli utenti. In tre mesi la "spam box" francese ha ricevuto 325 000 messaggi. Un'esperienza simile ha dato luogo, in Belgio, a 50 000 reclami in due mesi e mezzo<sup>1</sup>. La "spam box" permanente gestita dalla FTC, detta UCE Database, ha ricevuto 130 000 reclami al giorno all'inizio del 2003<sup>1</sup>.

Lo spam ha raggiunto un livello tale da rappresentare un fattore di costo importante per le imprese. In termini di costi diretti il personale deve ripulire le mailbox dai messaggi spam con conseguenze negative sull'efficienza e la produttività sul lavoro. I servizi informatici delle imprese consacrano tempo e denaro alla soluzione di questi problemi. I fornitori di servizi Internet (ISP) e i fornitori di servizi di posta elettronica (ESP) devono acquistare maggiore larghezza di banda e maggiore capacità per lo stoccaggio di messaggi elettronici indesiderati. Vi è inoltre il rischio che lo spam dia luogo alla responsabilità di chi lo riceve (ad es. contenuti nocivi sui computer dei dipendenti) o semplicemente – e involontariamente – lo ritrasmette (inserimento indebito della persona in una lista nera o danni alla sua reputazione). Lo spam genera anche costi indiretti:

<sup>6</sup> Stando ad una recente relazione della FTC, il 22% dello spam esaminato conteneva informazioni errate nella rubrica "soggetto" del messaggio; il 42% conteneva informazioni ingannevoli nella rubrica "soggetto" secondo le quali esisteva un legame commerciale o personale tra il mittente e il destinatario; il 44% conteneva informazioni errate nella rubrica "mittente" o "oggetto"; oltre la metà dello spam con finalità finanziaria conteneva informazioni errate nella rubrica "mittente" o "oggetto"; il 40% dello spam conteneva indicazioni errate nel testo del messaggio; il 90% dello spam relativo ad opportunità di investimento e commerciali conteneva affermazioni false; il 66% dello spam conteneva informazioni false nelle rubriche "mittente", "oggetto" o nel testo del messaggio. (False Claims in Spam, A report by the FTC's Division of Marketing Practices, 30 aprile 2003: <http://www.ftc.gov/reports/spam/030429spamreport.pdf>)

<sup>7</sup> Secondo Pew Internet, il 7% degli utenti di posta elettronica ha ordinato articoli a seguito di una e-mail non richiesta e il 33% di essi ha cliccato su un *link* di una e-mail non richiesta per ottenere ulteriori informazioni. Anche se la percentuale di consumatori truffati è relativamente bassa, il problema ha acquisito una dimensione nuova a causa delle eccezionali economie di scala che possono essere ottenute dagli operatori senza scrupoli ricorrendo a messaggi di spam fuorvianti o ingannevoli. Cfr. 'Spam-How It Is Hurting Email and Degrading Life on the Internet', ottobre 2003', Report by Deborah Fallows for the Pew Internet & American Life Project. La relazione è consultabile al seguente indirizzo:

[http://www.pewinternet.org/reports/pdfs/PIP\\_Spam\\_Report.pdf](http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf)

Un "bulk e-mailer" (ossia un mittente di e-mail di massa indiscriminate) ha recentemente dichiarato, in occasione dello "Spam Forum" organizzato dalla FTC nei mesi di aprile e maggio 2003, che la pratica è redditizia anche se il tasso di risposta è inferiore a 0,0001%. (Osservazioni di Timothy J. Muris Chairman, Federal Trade Commission, Aspen Summit, *Cyberspace and the American Dream*, The Progress and Freedom Foundation, 19 agosto 2003, Aspen, Colorado).

<sup>8</sup> I messaggi di spam contengono talvolta forme di violenza gratuita o di incitamento all'odio basato sulla razza, il sesso, la religione o la nazionalità.

alcune e-mail commerciali o professionali lecite non possono essere trasmesse a causa dei filtri antispam installati (fenomeno dei ‘falsi positivi’), o semplicemente non vengono lette perché associate a messaggi spam. Lo spam è inoltre utilizzato come vettore principale per la diffusione di virus, che possono rivelarsi estremamente costosi per le imprese.

È difficile calcolare il costo dello spam, in particolare per i privati, soprattutto perché è difficile quantificare il valore monetario di alcuni danni. Nondimeno, le stime sono generalmente preoccupanti. Ad esempio, Ferris Research ha stimato che nel 2002 lo spam è costato alle imprese europee 2,5 miliardi di euro in termini di calo della produttività<sup>9</sup>. Inoltre, come abbiamo visto poc’anzi, il volume di spam è considerevolmente aumentato dal 2002. Il produttore di software MessageLabs Ltd ha stimato che nel giugno 2003 il costo dello spam per le imprese britanniche è ammontato a 3,2 miliardi di sterline<sup>10</sup>. Lo spam può inoltre avere conseguenze diverse in funzione del settore colpito. Le imprese che operano in campo giuridico, ad esempio, possono subire notevoli pregiudizi a causa del carattere riservato e sensibile delle informazioni che trattano.

Una delle conseguenze più preoccupanti dello spam è il fatto che intacca la fiducia degli utenti, una delle condizioni essenziali per il successo del commercio elettronico e della società dell’informazione in generale. Il fatto che un canale di vendita al dettaglio sia considerato in preda ai truffatori può incidere negativamente sulla reputazione degli operatori onesti dello stesso settore. Dati recenti relativi agli Stati Uniti, che hanno maggiore esperienza dell’UE in materia di spam, confermano che la fiducia di molti consumatori nei confronti dell’e-mail è in calo a causa del gran numero di spam che ricevono<sup>11</sup>.

In termini generali, Internet e gli altri mezzi di comunicazione elettronica – accesso a banda larga, accesso senza filo – sono destinati a diventare i fattori essenziali dell’aumento della produttività delle economie moderne. Tuttavia, alcune delle caratteristiche di maggior richiamo di questi servizi – l’accesso permanente, l’accesso senza filo – rischiano di essere, in mancanza di adeguate misure di sicurezza, proprio i vettori di un considerevole aumento dello spam ricevuto e ritrasmesso. Si produrrebbe così un effetto perverso: la crescita di tali servizi causerebbe un aumento dello spam, a meno che non vengano rapidamente messe in atto efficaci misure di protezione.

## **2. SINTESI DELLE NORME CHE DISCIPLINANO LE COMUNICAZIONI COMMERCIALI INDESIDERATE**

### **2.1. Regime del consenso preliminare (“opt-in”)**

La direttiva 2002/58/CE relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche (la cui data di attuazione era il 31 ottobre 2003) stabilisce che gli Stati membri vietino l’invio di messaggi commerciali indesiderati mediante posta

---

<sup>9</sup> Fonte: Ferris Research, 2003.

<sup>10</sup> Questi dati ed altre stime provengono da “*Spam: Report of an Inquiry by the All Party Internet Group*”, Londra, ottobre 2003, pag. 8. La relazione può essere consultata al seguente indirizzo: <http://www.apig.org.uk>

<sup>11</sup> Stando alla recente indagine di Pew Internet menzionata in precedenza, il 25% degli intervistati ha ridotto l’uso dell’e-mail a causa del grande volume di spam ricevuto.

elettronica o altri sistemi di messaggeria elettronica quali SMS o MMS (*Multimedia Messaging Service*) a meno che l'abbonato al servizio di comunicazione elettronica non abbia preventivamente espresso il suo consenso (articolo 13, paragrafo 1 della direttiva)<sup>12</sup>. È in questo che consiste il cosiddetto regime "opt-in", finora applicabile solo ai telefax e ai dispositivi di chiamata automatici<sup>13</sup>.

**Le tre regole di base del nuovo regime:**

**Regola n. 1:** Le attività di marketing diretto per posta elettronica sono soggette al consenso preliminare degli abbonati. È prevista un'eccezione di portata limitata per le e-mail (o gli SMS) inviati da un'impresa ai propri clienti per proporre servizi o prodotti analoghi. Questo regime si applica nei confronti degli abbonati quando questi sono persone fisiche, ma gli Stati membri possono decidere di estenderlo alle persone giuridiche.

**Regola n. 2:** È illecito camuffare o mascherare l'identità del mittente a nome del quale viene effettuata la comunicazione.

**Regola n. 3:** Tutti i messaggi di posta elettronica devono contenere un indirizzo di risposta valido al quale l'abbonato può chiedere che non gli vengano più inviati messaggi.

Non tutte le e-mail non richieste sono vietate. È prevista una deroga per i casi in cui l'indirizzo e-mail o SMS è stato ottenuto nel contesto di una vendita. Si parla in questi casi di "soft opt-in". Nel quadro delle relazioni con la clientela l'impresa che ha ottenuto i dati dai propri clienti può utilizzarli per la vendita diretta di prodotti o servizi analoghi a quelli già venduti a tali clienti. Questa deroga è stata armonizzata a livello comunitario e gli Stati membri non possono che darvi attuazione. La deroga deve tuttavia essere formulata in modo restrittivo in modo da non pregiudicare il regime "opt-in". Anche in questo caso, tuttavia, l'impresa è tenuta ad indicare chiaramente, al momento della raccolta dei dati, che questi potranno essere utilizzati per fini di marketing diretto (e, ove necessario, trasmessi a terzi a tal fine) e a permettere al cliente di opporsi "gratuitamente e in maniera agevole". Inoltre, ogni successivo messaggio di marketing diretto deve permettere al cliente di far cessare in modo semplice e gratuito l'invio di nuovi messaggi (regime "opt-out").

Il sistema "opt-in" è obbligatorio per tutte le e-mail e gli SMS inviati a persone fisiche per fini di vendita diretta. Gli Stati membri possono estendere l'applicazione di questo sistema ai messaggi destinati alle imprese (persone fisiche). Gli Stati membri che hanno adottato un regime "opt-out" per le comunicazioni tra imprese (*business-to-business*) con relative "liste di esclusione" possono continuare ad applicare lo stesso sistema. L'applicazione di un regime diverso in funzione della natura (privato o impresa) di un abbonato ad un servizio di posta elettronica potrebbe causare difficoltà ai mittenti, non sempre in grado di distinguere tra persone fisiche e giuridiche.

Per tutte le categorie di destinatari (persone fisiche o giuridiche) la direttiva vieta l'invio di messaggi di marketing diretto in cui l'identità del mittente sia mascherata o nascosta.

---

<sup>12</sup> Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) GU L 201 del 31.7.2002.

<sup>13</sup> Per i messaggi di prospezione commerciale telefonica gli Stati membri possono scegliere tra l'approccio "opt-in" e l'approccio "opt-out".

Tali messaggi devono altresì contenere un indirizzo di risposta valido al quale il destinatario possa chiedere la cessazione dei messaggi<sup>14</sup>.

Il gruppo di lavoro “Articolo 29 – protezione dati”, istituito per assistere la Commissione, riunisce esponenti delle autorità responsabili della protezione dati nell’UE e sta esaminando alcuni di questi concetti con maggiore attenzione al fine di contribuire ad un’applicazione uniforme delle misure nazionali adottate in virtù della direttiva 2002/58/CE<sup>15</sup>. Raggiungere un consenso in merito a questi aspetti eviterà divergenze interpretative che potrebbero nuocere al funzionamento del mercato interno. Precedenti documenti del gruppo di lavoro trattano altri aspetti legati alle comunicazioni indesiderate<sup>16</sup>.

## 2.2. Disposizioni esecutive

Le disposizioni della direttiva “generale” sulla protezione dati in materia di ricorso giurisdizionale, responsabilità e sanzioni si applicano anche alle disposizioni della direttiva sulla protezione della vita privata nel settore delle comunicazioni elettroniche, comprese le disposizioni relative alle comunicazioni indesiderate<sup>17</sup>.

Gli Stati membri devono provvedere affinché in caso di infrazione sia previsto un regime di ricorso e di sanzioni. Ogni violazione dei diritti stabiliti dal diritto interno deve dar luogo ad un diritto individuale al ricorso giurisdizionale. Benché il ricorso giurisdizionale faccia salvo un eventuale (e precedente) ricorso amministrativo, non esistono requisiti di armonizzazione per tali procedure amministrative. Ogni danno subito a causa di un trattamento o di un atto illegale deve dar luogo ad un diritto individuale al risarcimento.

---

<sup>14</sup> Articolo 13, paragrafo 4 della direttiva 2002/58/CE.

<sup>15</sup> Conformemente all’articolo 15, paragrafo 3 della direttiva 2002/58/CE, in combinato disposto con l’articolo 30 della direttiva 95/46/CE.

<sup>16</sup> Cfr. ad esempio il parere 7/2000 sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2000; raccomandazione 2/2001 su alcuni requisiti minimi per la raccolta online di dati personali nell’Unione europea. La raccolta automatica di dati è stata esaminata anche nel documento di lavoro del 21 novembre 2000 intitolato “Tutela della vita privata su Internet - Un approccio integrato dell’UE alla protezione dei dati on-line”. Tali documenti possono essere consultati al seguente indirizzo:  
[http://europa.eu.int/comm/internal\\_market/privacy/workinggroup\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/workinggroup_en.htm)

<sup>17</sup> L’articolo 15 della direttiva 2002/58/CE rimanda al capo III della direttiva 95/46/CE “Ricorsi giurisdizionali, responsabilità e sanzioni”:

### Articolo 22 – Ricorsi

Fatti salvi ricorsi amministrativi che possono essere promossi, segnatamente dinanzi all’autorità di controllo di cui all’articolo 28, prima che sia adita l’autorità giudiziaria, gli Stati membri stabiliscono che chiunque possa disporre di un ricorso giurisdizionale in caso di violazione dei diritti garantitigli dalle disposizioni nazionali applicabili al trattamento in questione.

### Articolo 23 – Responsabilità

1. Gli Stati membri dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente direttiva abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento.

2. Il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l’evento dannoso non gli è imputabile.

### Articolo 24 – Sanzioni

Gli Stati membri adottano le misure appropriate per garantire la piena applicazione delle disposizioni della presente direttiva e in particolare stabiliscono le sanzioni da applicare in caso di violazione delle disposizioni di attuazione della presente direttiva.

Ogni infrazione deve inoltre dar luogo a sanzione, in modo da garantire la piena applicazione della direttiva.

In altri termini, se, da un lato, la natura stessa di una direttiva garantisce agli Stati membri un certo margine di manovra circa la scelta delle misure da adottare per darvi attuazione – compresi ricorsi e sanzioni –, dall'altro, tali misure sono necessarie per garantire la piena attuazione delle disposizioni in materia di comunicazioni commerciali indesiderate.

Come generalmente avviene per le direttive, la responsabilità dell'applicazione delle norme incombe in primo luogo agli Stati membri e non alla Commissione. Ad esempio, non spetta alla Commissione perseguire o imporre sanzioni pecuniarie a coloro che violano i diritti e gli obblighi stabiliti dalla direttiva<sup>18</sup>.

### **2.3. Altre disposizioni applicabili in materia di spam**

Una pratica spesso correlata a quella dello spam è la raccolta di indirizzi e-mail, ossia la raccolta automatica di dati personali presso siti Internet pubblici (web, *chatroom* ecc.). Si tratta di una pratica vietata dalla direttiva “generale” 95/46/CE sulla protezione dei dati, a prescindere dal fatto che la raccolta avvenga o meno automaticamente per mezzo di un apposito software<sup>19</sup>.

Lo spam fraudolento e ingannevole può essere particolarmente offensivo. Queste pratiche sono già considerate illegali ai sensi della vigente normativa UE sulla pubblicità ingannevole e le prassi commerciali sleali (ad es. la direttiva 84/450/CEE sulla pubblicità ingannevole)<sup>20</sup>. In genere anche le legislazioni nazionali prevedono pene più severe per i casi più gravi, e talvolta sanzioni penali.

Talune categorie di spam possono risultare ancora più scioccanti, come i messaggi di carattere pornografico o contenenti immagini di violenza gratuita, soprattutto quando sono i bambini ad esservi esposti<sup>21</sup>. Malgrado i contenuti di alcuni di questi messaggi siano nocivi ma non necessariamente illegali, la loro diffusione indiscriminata ad adulti e minori è generalmente considerata illegale dalla legge nazionale e può talvolta comportare pene severe. I messaggi di spam possono anche avere contenuti illegali quali incitamenti all'odio per motivi legati alla razza, al sesso, alla religione o alla nazionalità. In ogni caso, dal momento in cui questi messaggi presentano fini di vendita diretta – come del resto spesso accade – essi sono soggetti al divieto di spam come le altre categorie di e-mail indesiderate.

---

<sup>18</sup> Situazione diversa da quella di agenzie come la *Federal Trade Commission* statunitense.

<sup>19</sup> Cfr. anche il documento di lavoro del “gruppo per la tutela dei dati personali (articolo 29)” dal titolo “Tutela della vita privata su Internet - Un approccio integrato dell'UE alla protezione dei dati on-line” (WP 37, adottato il 21 novembre 2000).

<sup>20</sup> Direttiva 84/450/CEE del Consiglio del 10 settembre 1984 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di pubblicità ingannevole, GU L 250 del 19.9.1984, pagg. 17-20. La Commissione ha recentemente presentato una proposta di sostituzione e aggiornamento della direttiva sulla pubblicità ingannevole (COM(2003) 356 def.).

<sup>21</sup> Il 24 settembre 1998 il Consiglio ha adottato la raccomandazione concernente lo sviluppo della competitività dell'industria dei servizi audiovisivi e d'informazione europei attraverso la promozione di strutture nazionali volte a raggiungere un livello comparabile e efficace di tutela dei minori e della dignità umana (98/560/CE). Si tratta del primo strumento giuridico comunitario riguardante i contenuti dei servizi audiovisivi e d'informazione che comprende tutte le modalità di erogazione, dalla radiodiffusione a Internet.

Occorre inoltre far riferimento all'obbligo, stabilito dalla direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (direttiva sul commercio elettronico), che le "comunicazioni commerciali" siano chiaramente identificabili come tali (cfr. articolo 6, lettera a) della direttiva sul commercio elettronico)<sup>22</sup>.

Inoltre, atti illeciti quali la pirateria informatica o il furto di identità sono spesso finalizzati allo spam (inviare messaggi di spam o accedere a database di indirizzi o a computer). Molte di queste attività rientrano nel campo di applicazione della decisione quadro sugli attacchi ai sistemi informatici, che prevede anche sanzioni di tipo penale. La decisione quadro, basata su una proposta della Commissione, è stata oggetto di un accordo politico nel febbraio 2003 e dovrebbe essere presto ufficialmente adottata<sup>23</sup>. In numerosi Stati membri l'accesso illecito a un server o a un PC o il loro utilizzo abusivo sono già perseguibili come reati penali.

### **3. ATTUAZIONE ED APPLICAZIONE EFFICACI DA PARTE DEGLI STATI MEMBRI E DELLE PUBBLICHE AUTORITÀ**

Questo capitolo descrive le azioni proposte che dovranno essere poste in essere dai governi e dalle pubbliche autorità degli Stati membri, in particolare in materia di ricorsi e sanzioni, meccanismi di reclamo (anche transfrontalieri), cooperazione con i paesi terzi e monitoraggio.

Prima di esaminare la questione dell'applicazione, la Commissione rileva che un certo numero di Stati membri non ha ancora recepito la direttiva sulla protezione della vita privata nel settore delle comunicazioni elettroniche, in particolare le disposizioni sulle e-mail commerciali indesiderate, che fa parte di un più ampio quadro normativo per le comunicazioni elettroniche<sup>24</sup>. Il Parlamento europeo ha di recente espresso la propria preoccupazione per questo ritardo<sup>25</sup>. A seguito della scadenza del termine di attuazione

---

<sup>22</sup> Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("direttiva sul commercio elettronico"), GU L 178 del 17.7.2000. Di norma le "comunicazioni commerciali" devono essere compatibili con le pertinenti norme vigenti nello Stato membro in cui è stabilito il prestatore del servizio. Questa regola non si applica tuttavia all'ammissibilità delle comunicazioni commerciali non sollecitate per posta elettronica (cfr. articolo 3 e allegato della direttiva). Nei casi (limitati) in cui le persone fisiche non siano tutelate dalla direttiva 2002/58/CE (ad es. persone fisiche che non sono abbonati) contro le comunicazioni commerciali non richieste, gli Stati membri devono inoltre provvedere, ai sensi della direttiva sul commercio elettronico, affinché i prestatori di servizi che inviano comunicazioni commerciali non richieste per posta elettronica consultino regolarmente e rispettino i registri negativi (registri "opt-out") in cui possono iscriversi le persone fisiche che non desiderano ricevere tali comunicazioni commerciali. (cfr. articolo 7 della direttiva sul commercio elettronico).

<sup>23</sup> Proposta di decisione-quadro del Consiglio relativa agli attacchi contro i sistemi di informazione, COM(2002) 173 def del 19.4.2002.

<sup>24</sup> Cfr. anche la nona relazione sull'applicazione del pacchetto normativo sulle telecomunicazioni consultabile al seguente indirizzo:  
[http://europa.eu.int/information\\_society/topics/ecommerce/all\\_about/implementation\\_enforcement/annualreports/9threport/index\\_en.htm](http://europa.eu.int/information_society/topics/ecommerce/all_about/implementation_enforcement/annualreports/9threport/index_en.htm)

<sup>25</sup> Nella comunicazione "Comunicazioni elettroniche: verso l'economia della conoscenza" la Commissione sottolinea l'importanza di una piena, efficace e puntuale attuazione del nuovo quadro normativo per le comunicazioni elettroniche e in particolare della direttiva sulla tutela della vita privata nel settore delle comunicazioni elettroniche (COM(2003) 65 dell'11 febbraio 2003).

della direttiva sulla protezione della vita privata nel settore delle comunicazioni elettroniche, fissato al 31 ottobre 2003, nel mese di novembre 2003 la Commissione ha avviato procedimenti di infrazione nei confronti di diversi Stati membri per mancata notifica delle misure di attuazione<sup>26</sup>.

### 3.1. Introduzione

Per quanto la legislazione possa agire da deterrente nei confronti dello spam, non basterà, da sola, ad arginare il fenomeno. Gli Stati membri devono garantire prioritariamente un'applicazione efficace del regime "opt-in". Oltre alla disponibilità di personale e risorse sufficienti, ciò richiede adeguati meccanismi di controllo dell'applicazione, anche a livello transfrontaliero. È indispensabile inoltre una stretta cooperazione con i paesi terzi. Altrettanto importanti sono le attività di monitoraggio, quanto meno per definire le priorità sulle quali orientare le attività di controllo dell'applicazione.

Diversi fattori sembrano incidere sull'efficacia dei meccanismi di applicazione:

- possibilità di far applicare la legislazione mediante efficaci sanzioni pecuniarie o di altro tipo. Sembra che alcune autorità di regolamentazione non dispongano ancora di (effettivi) poteri coercitivi;
- natura dei meccanismi di reclamo e di ricorso a disposizione delle persone fisiche e giuridiche;
- necessità di chiarezza e di coordinamento tra le autorità nazionali a causa della frequente sovrapposizione di competenze in questo settore;
- consapevolezza degli utenti in merito ai loro diritti e al modo di esercitarli. Gli utenti devono essere informati circa il luogo dove sporgere reclamo, i fatti che possono essere oggetto di indagine, le azioni esecutive che possono essere adottate e le informazioni da fornire alle autorità perché un'indagine possa essere aperta;
- coordinamento e cooperazione tra gli Stati membri e tra gli Stati membri e i paesi terzi sul diritto applicabile in fattispecie specifiche;
- risorse disponibili per individuare gli *spammer* che operano nell'UE o in paesi terzi e mascherano la loro identità, anche mediante l'usurpazione di altre identità, indirizzi o server.

Le misure applicabili ai fini dell'esecuzione delle disposizioni sulle comunicazioni indesiderate sono state descritte nel capitolo 2.2. Le procedure relative alle e-mail commerciali indesiderate sono state fin qui strutturate e gestite in modo piuttosto disomogeneo dai vari paesi<sup>27</sup>. Malgrado la scelta di uno strumento come la direttiva implichi che gli Stati membri dispongono di un certo margine di manovra per quanto riguarda l'attuazione delle sue disposizioni, è indispensabile un efficace meccanismo di applicazione, a prescindere dal metodo utilizzato.

---

<sup>26</sup> Le lettere di costituzione in mora sono state inviate il 25 novembre 2003 (cfr. IP/03/1663).

<sup>27</sup> Va sottolineato che i reclami riguardano spesso anche altri aspetti, ad es. il diritto di accesso ai dati personali e il diritto di opporsi ad un trattamento.

### Situazioni diverse negli Stati membri

Il controllo dell'applicazione delle disposizioni in materia di comunicazioni commerciali indesiderate non è demandato alle stesse autorità in tutti gli Stati membri. Nella maggior parte dei casi è l'autorità preposta alla protezione dei dati ad avere la responsabilità primaria. In altri paesi, tuttavia, questo compito spetta alle autorità nazionali di regolamentazione per le comunicazioni elettroniche (ANR). In altri ancora, l'applicazione delle norme spetta alle autorità per la protezione dei consumatori (compreso il mediatore dei consumatori). Spesso occorre coinvolgere più di un'autorità nell'applicazione delle disposizioni sulle comunicazioni commerciali indesiderate. Inoltre, lo spam è spesso accompagnato da pratiche ingannevoli o fraudolente. (Una minoranza di Stati membri non si è dotata di un'autorità di protezione dei consumatori e l'applicazione delle norme è lasciata alle associazioni di tutela dei consumatori o ai singoli consumatori). Spesso, lo spam è legato anche ad infrazioni delle disposizioni sulla protezione dei dati (come la raccolta di indirizzi elettronici) se non addirittura ad atti di criminalità informatica (quali l'accesso illegale a PC o server). Non sempre sono le stesse autorità ad applicare le corrispondenti disposizioni, a maggior ragione a livello transfrontaliero.

Salvo in alcuni Stati membri, i reclami non danno sistematicamente luogo ad un'indagine. Si ricorre talvolta con un certo successo a soluzioni "preventive" ossia ad indirizzi, consigli e orientamenti alle imprese per evitare che cadano nell'infrazione. In alcuni casi questa fase "pre-reclamo" è lasciata al consumatore, tenuto a contattare l'impresa prima di sporgere il reclamo. Alcuni paesi hanno istituito sistemi di autoregolamentazione (ad es. il Regno Unito) per strutturare questa prima fase di azione. In altri l'industria ha posto in essere meccanismi di reclamo e autoregolamentazione. Le autorità agiscono spesso di propria iniziativa. L'attribuzione di competenze in questo campo ad un'autorità amministrativa non esclude di norma un accesso diretto al ricorso giurisdizionale.

Non tutte le autorità per la protezione dei dati possono perseguire persone giuridiche, così come non tutte – almeno finora – possono imporre sanzioni. Esse devono adire l'autorità giudiziaria perché avvii un procedimento. In Francia, l'esperienza con le mailbox elettroniche ha spinto l'autorità per la protezione dei dati a scegliere alcuni casi e a deferirli all'autorità giudiziaria, senza grande successo. In Belgio, un'esperienza analoga ha consentito uno scambio di vedute con i presunti mittenti degli spam e, nei casi transfrontalieri, al loro deferimento alle autorità competenti degli Stati membri dell'UE o alla FTC degli Stati Uniti.

Un approccio equilibrato basato sulla legislazione, il controllo dell'applicazione delle norme e l'autoregolamentazione è considerato il modo migliore per garantire l'applicazione del regime "opt-in". Gli Stati membri sono invitati a valutare l'efficacia dei rispettivi sistemi di applicazione, in particolare alla luce delle varie azioni proposte di seguito (cfr. punti da 3.2 a 3.6).

Gli Stati membri sono inoltre invitati a definire strategie nazionali per garantire la cooperazione tra le autorità per la protezione dati, le autorità di tutela dei consumatori e le autorità nazionali di regolamentazione per le comunicazioni elettroniche (ANR) e ad evitare sovrapposizioni e ridondanze di competenze tra tali organismi.

Per agevolare e coordinare gli scambi di informazioni e di migliori pratiche sulle modalità efficaci di controllo dell'applicazione delle norme (ad esempio in materia di reclami, ricorsi giurisdizionali, sanzioni, cooperazione internazionale) i servizi della Commissione hanno istituito un **gruppo informale online sulle comunicazioni commerciali indesiderate** con l'ausilio degli Stati membri e delle autorità per la protezione dei dati. Il gruppo di lavoro faciliterà e coordinerà le attività nel quadro delle altre azioni individuate nella presente comunicazione, ossia la sensibilizzazione e le soluzioni tecniche.

I documenti elaborati a seguito delle discussioni del gruppo di lavoro saranno generalmente sottoposti al comitato per le comunicazioni (COCOM) istituito ai sensi del quadro normativo per le reti e i servizi di comunicazione elettronica e/o al gruppo di lavoro “Articolo 29 – protezione dati” perché decidano le azioni da intraprendere. Il gruppo potrà in particolare definire i criteri di valutazione comparativa a cui sottoporre le varie misure proposte.

Il gruppo di lavoro online si compone di rappresentanti delle competenti amministrazioni nazionali, delle autorità per la protezione dati e della Commissione e deciderà le modalità di partecipazione di altre parti interessate.

## **3.2. Ricorsi e sanzioni efficaci**

### *3.2.1. Discussione*

Al momento le soluzioni consistono generalmente in sanzioni pecuniarie o in ingiunzioni di cessazione del trattamento illegale dei dati, corredate talvolta della disattivazione dei siti interessati. In taluni Stati membri l'ingiunzione di cessazione precede o è contestuale alla sanzione pecuniaria in caso di mancato adempimento. Tuttavia, non tutte le autorità hanno competenza giurisdizionale sull'insieme delle infrazioni legate allo spam né dispongono tutte degli stessi strumenti. Spesso il caso viene deferito all'autorità giudiziaria. Non tutti gli Stati membri, tuttavia, hanno previsto sanzioni giudiziarie per questo tipo di infrazioni.

Non tutti gli Stati membri prevedono vie di ricorso e multe/sanzioni nel loro diritto amministrativo o penale. Le sanzioni penali variano da uno Stato membro e l'altro e prevedono talvolta pene detentive. È inoltre possibile, generalmente, ottenere un risarcimento danni ricorrendo al tribunale civile.

Benché esista di norma una distinzione tra infrazioni lievi e infrazioni gravi (ad es. mailing indiscriminato, pubblicità e pratiche commerciali ingannevoli o fraudolente), anche le sanzioni variano notevolmente in funzione degli Stati membri.

In molte circostanze le attività di spam permettono di esperire le vie di ricorso previste dalla legislazione generale sulla protezione dei dati (ad es. inosservanza dell'obbligo di notifica, violazione del diritto di accesso, inosservanza dell'obbligo di designare un rappresentante in uno Stato membro ecc.) o dalla legislazione specifica (ad es. pubblicità ingannevole, pratiche commerciali fraudolente ecc.). Prima che venisse posto in essere il regime “opt-in” si è fatto ricorso ad argomentazioni giuridiche di diversi tipi per contrastare alcune forme di spam (campagne indiscriminate di promozione per posta elettronica, uso illecito di dati personali, interruzione della rete, usurpazione di indirizzi e-mail, frode e interpretazione erronea dei contratti).

In termini generali il ricorso giurisdizionale non è considerato una forma sufficiente di controllo dell'applicazione. Di norma le sanzioni pecuniarie amministrative possono essere inflitte dall'autorità per la protezione dati, dall'autorità per la protezione dei consumatori e/o dall'ANR, ma i loro importi variano. Gli Stati membri che non dispongono di questo meccanismo prevedono di introdurlo. Rispetto alle soluzioni giudiziarie, le sanzioni amministrative sembrano particolarmente adeguate a questo settore dinamico. Le autorità per la protezione dati, le autorità per la protezione dei consumatori e le ANR fanno spesso ricorso a strumenti complementari per garantire

l'applicazione delle norme. Le procedure amministrative possono risultare poco costose e rapide (non oltre 50 giorni, stando all'autorità per la protezione dati italiana).

### *3.2.2. Azioni proposte*

Come condizione indispensabile, la Commissione esorta gli Stati membri che non hanno ancora recepito la direttiva e in particolare le disposizioni relative alle comunicazioni indesiderate, a procedervi senza ulteriori ritardi. I servizi della Commissione sono disposti, ove necessario, ad assistere gli Stati membri.

Gli Stati membri sono invitati a valutare l'efficacia dei rispettivi meccanismi di ricorso e di sanzione in caso di infrazione e ad offrire alle vittime adeguate possibilità di ottenere risarcimento.

Gli Stati membri e le autorità competenti che non dispongono di vie di ricorso amministrativo sono invitate ad introdurre questo tipo di soluzioni contro lo spam al fine di garantire procedure rapide, poco costose ed efficaci di applicazione del regime "opt-in".

La Commissione si accerterà che le misure di attuazione nazionali prevedano sanzioni effettive in caso di inosservanza degli obblighi da parte degli operatori del mercato, comprese, ove opportuno, sanzioni pecuniarie e penali.

In tale contesto la Commissione accerterà anche che le autorità competenti dispongono dei necessari poteri investigativi ed esecutivi.

## **3.3. Meccanismi di reclamo**

### *3.3.1. Discussione*

Perché le norme siano applicate efficacemente occorre disporre di adeguati meccanismi di reclamo. Talune autorità per la protezione dati hanno messo a disposizione appositi indirizzi di posta elettronica ai quali gli utenti possono inoltrare le e-mail commerciali indesiderate e si sono impegnate ad intervenire in casi specifici.

Alcuni Stati membri sembrano preferire procedure amministrative ordinarie e/o contatti con gli ISP o con i team di intervento in caso di emergenza informatica (CERT) se si verificano perturbazioni della rete. Altri Stati membri ricorrono invece a procedure più tradizionali (azioni di risarcimento danni secondo il diritto civile/amministrativo). Coregolamentazione e autoregolamentazione sono talvolta considerate alternative preferibili alle misure di esecuzione diretta.

### **Migliori pratiche**

Alla fine del 2002 la Francia e il Belgio hanno messo a disposizione indirizzi elettronici dedicati ai quali il pubblico era invitato ad inviare reclami precisi in materia di spam. I risultati dell'esperienza sono interessanti. Le relazioni elaborate a seguito dell'iniziativa sono disponibili al pubblico<sup>28</sup>. La Francia prevede di utilizzare questo sistema permanentemente nel quadro delle nuove norme di attuazione della direttiva sulla protezione dei dati nel settore delle comunicazioni elettroniche. La *Federal Trade Commission* (FTC), negli Stati Uniti, utilizza una mailbox simile e utilizza i messaggi in entrata per perseguire le pratiche commerciali sleali e ingannevoli<sup>29</sup>.

Le mailbox elettroniche hanno il vantaggio di incoraggiare i consumatori a denunciare le infrazioni, rendendo quindi più efficace l'applicazione della legislazione. Le mailbox possono inoltre fornire statistiche essenziali sulla portata e la natura del problema in un determinato paese o regione. Forniscono così una panoramica chiara della situazione che costituisce per le autorità uno strumento prezioso per fissare o adattare le priorità in materia di controllo dell'applicazione. Inoltre, grazie ai dati così acquisiti, possono essere messe in atto azioni preventive. La CNIL (l'autorità francese per la protezione dei dati) ha utilizzato i dati raccolti nel corso dell'operazione "boîte à spam" per elaborare fascicoli informativi di prevenzione destinati agli utenti ed ai responsabili del marketing.

L'utilità di una mailbox elettronica per sorvegliare e misurare la portata ed il campo di applicazione dello spam dipende naturalmente dalla capacità di indagare efficacemente e rapidamente in merito ai reclami presentati.

Benché si osservi un interesse generale per l'esperienza acquisita da altri Stati membri grazie a questo metodo, rari sono gli Stati membri che sembrano prevedere la possibilità di utilizzare una mailbox elettronica dedicata. Le ragioni indicate sono generalmente il fatto che esista già la possibilità di introdurre un reclamo per posta elettronica, di norma sul sito web dell'autorità; la necessità di disporre di personale specializzato e di risorse supplementari e infine l'obbligo di modificare le procedure giuridiche.

### *3.3.2. Azioni proposte*

Gli Stati membri e le autorità competenti devono valutare la capacità dei rispettivi ordinamenti giuridici di esaminare i reclami degli utenti e provvedere ad eventuali adattamenti.

Gli Stati membri e le autorità competenti sono invitati a mettere in servizio mailbox elettroniche dedicate e a sostenerne il lancio mediante opportune campagne d'informazione.

Queste mailbox dedicate devono essere concepite in modo tale da facilitare la ricerca e l'analisi dei dati al fine di migliorare la comprensione del problema e fissare priorità in materia di misure di controllo dell'applicazione della legislazione.

<sup>28</sup> La relazione adottata il 24 ottobre 2002 dall'autorità per la protezione dati francese *Commission Nationale Informatique et Libertés* (CNIL) è consultabile al seguente indirizzo:

[http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam\\_sommaire.htm](http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm)

La relazione del luglio 2003 dell'autorità per la protezione dati belga *Commission de Protection de la Vie Privée* è consultabile al seguente indirizzo:

[http://www.privacy.fgov.be/publications/spam\\_4-7-03\\_fr.pdf](http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf)

<sup>29</sup> Cfr. ad es. <http://www.ftc.gov/bcp/online/pubs/online/inbox.pdf> I messaggi indesiderati o ingannevoli possono essere trasmessi al seguente indirizzo: [uce@ftc.gov](mailto:uce@ftc.gov)

I servizi della Commissione faciliteranno lo scambio di informazioni sulle esperienze acquisite dagli Stati membri con le mailbox elettroniche.

### **3.4. Reclami transfrontalieri e cooperazione in materia di controllo dell'applicazione all'interno dell'UE**

#### *3.4.1. Discussione*

Il trattamento efficace dei reclami transfrontalieri contribuisce a garantire un'effettiva tutela dei consumatori in questo settore. In ogni caso, è indispensabile collegare tra loro i meccanismi di reclamo nazionali, indipendentemente dalle loro modalità di funzionamento, in modo che i reclami presentati dagli utenti in uno Stato membro riguardanti messaggi provenienti da un altro Stato membro possano anch'essi essere trattati con la dovuta efficacia (cfr. punto 3.5 sulla cooperazione con i paesi terzi).

Non tutti gli Stati membri dispongono di procedure formali di esame dei reclami transfrontalieri. Le soluzioni attualmente utilizzate consistono nel contattare l'autorità competente di un altro Stato membro e nella possibilità di trasferire il reclamo all'autorità competente del paese di origine del o dei messaggi.

A livello europeo (paesi SEE e paesi candidati compresi), le autorità per la protezione dati procedono a scambi di informazioni in materia di reclami transfrontalieri nel quadro di un "gruppo di esame dei reclami" istituito nell'ambito della conferenza europea dei commissari incaricati della protezione dei dati. Il gruppo è competente per i reclami transfrontalieri relativi allo spam e in particolare per determinare il diritto applicabile in casi specifici. Va osservato, tuttavia, che non tutte le autorità per la protezione dati danno applicazione alle disposizioni sulle comunicazioni indesiderate.

Dal punto di vista della tutela dei consumatori, la Commissione ha recentemente presentato una proposta di regolamento in materia di cooperazione per la tutela dei consumatori che istituisce una rete di autorità pubbliche incaricate di trattare i problemi transfrontalieri<sup>30</sup>. La proposta di regolamento istituisce procedure di mutua assistenza e prevede una cooperazione operativa approfondita tra le autorità nazionali. Lo spam ingannevole, fuorviante o in contrasto con le altre norme sulla tutela dei consumatori rientrerebbe nel campo di applicazione del regime proposto, ma non tutto lo spam vietato ai sensi della direttiva sulla protezione della vita privata nel settore delle comunicazioni elettroniche. La proposta di regolamento è attualmente allo studio in sede di Consiglio e di Parlamento europeo.

#### *3.4.2. Azioni proposte*

Gli Stati membri e le autorità competenti sono invitati a valutare l'efficacia delle rispettive procedure di esame dei reclami transfrontalieri (accordi di mutua assistenza, ad esempio).

Si incoraggia il coordinamento delle azioni tra le amministrazioni nazionali competenti. Può trattarsi, in particolare, di attività di coordinamento e di scambio di informazioni tra autorità competenti per l'applicazione delle nuove disposizioni, e tra queste autorità e

---

<sup>30</sup> COM(2003) 443 def.

altre autorità competenti per forme particolari di spam (ad esempio, spam fraudolenti o “scams”, spam pornografici, messaggi sui prodotti di salute distribuiti illegalmente).

Per quanto riguarda gli spam fraudolenti ed ingannevoli, il Consiglio ed il Parlamento sono invitati ad approvare quanto prima la proposta di regolamento sulla cooperazione in materia di tutela dei consumatori affinché le autorità nazionali per la tutela dei consumatori dispongano di tutti gli strumenti necessari per contrastare gli spam ingannevoli e fuorvianti. Le due istituzioni sono inoltre invitate ad esaminare la possibilità di estendere il campo di applicazione di questo regolamento alla direttiva relativa alla protezione della vita privata nel settore delle comunicazioni elettroniche.

Gli Stati membri sono invitati ad esaminare in che modo eliminare gli ostacoli allo scambio di informazioni ed alla cooperazione nonché la possibilità di chiedere un intervento da parte delle autorità di altri Stati membri. Potrebbe essere utile al riguardo disporre di un meccanismo di collegamento (cfr. l'iniziativa delle autorità per la protezione dati menzionata in precedenza) nel quadro del quale le autorità di regolamentazione nazionali potrebbero cooperare ai fini di un'applicazione transfrontaliera delle norme. La costituzione di una rete di sostegno alla cooperazione potrebbe fondarsi su altri programmi della Commissione (ad es. il programma IDA<sup>31</sup>).

La Commissione intende facilitare e promuovere queste iniziative di coordinamento tra le autorità nazionali competenti, in particolare mediante il nuovo gruppo informale online sulle comunicazioni commerciali indesiderate. I servizi della Commissione hanno iniziato ad esaminare, di concerto con gli Stati membri e le autorità nazionali interessate all'applicazione di queste norme, le azioni concrete necessarie per migliorare l'esame dei reclami transfrontalieri. Le discussioni con le autorità nazionali proseguiranno nel corso del 2004.

### **3.5. Cooperazione con i paesi terzi**

#### *3.5.1. Discussione*

Le nuove norme si applicano ai dati a carattere personale elaborati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico sulle reti pubbliche di comunicazione nell'Unione europea (e nel SEE). Di conseguenza, l'articolo 13 della direttiva 2002/58/CE che stabilisce la norma del consenso preliminare (“opt-in”) si applica a tutte le comunicazioni commerciali indesiderate veicolate da e verso reti situate nell'Unione europea (e nel SEE). Ciò significa che anche i messaggi provenienti da paesi terzi devono essere conformi alle norme UE, alla stregua dei messaggi inviati dall'UE verso destinatari in paesi terzi.

L'applicazione effettiva della norma “opt-in” riguardo ai messaggi provenienti da paesi terzi sarà senza dubbio più complessa che per i messaggi provenienti dall'UE. Tale applicazione è tuttavia indispensabile in quanto gran parte dello spam ha origine al di fuori dell'Unione.

Sarà pertanto necessario disporre di un arsenale di strumenti diversi: misure di prevenzione, dispositivi di filtraggio, misure di autoregolamentazione, disposizioni

---

<sup>31</sup> Informazioni in merito al programma IDA possono essere ottenute al seguente indirizzo: <http://europa.eu.int/comm/enterprise/ida/index.htm>

contrattuali e misure di cooperazione internazionale. Il presente capitolo è dedicato alla cooperazione internazionale, il cui primo obiettivo è promuovere l'adozione di una legislazione efficace da parte dei paesi terzi. Il secondo obiettivo consiste invece nella cooperazione con i paesi terzi ai fini di garantire un'applicazione efficace delle norme adottate.

Non esiste una vera e propria esperienza in materia di applicazione delle norme di consenso preliminare (“opt-in”) e di opposizione (“opt-out”) per le comunicazioni aventi origine al di fuori dell'UE. Oltre al fatto che lo spam è un fenomeno relativamente nuovo, l'applicazione di tali norme si scontra anche con la difficoltà di identificare i mittenti o con gli sforzi necessari per giungere a tale identificazione; con la mancanza di (adeguati) meccanismi internazionali di cooperazione e con il fatto che talune autorità non abbiano giurisdizione sulle questioni internazionali.

Per quanto riguarda lo spam fraudolento e ingannevole, la proposta di regolamento della Commissione sulla cooperazione in materia di tutela dei consumatori prevede anche disposizioni in materia di cooperazione con i paesi terzi sull'applicazione delle norme. L'organizzazione per la cooperazione e lo sviluppo economici (OCSE) ha adottato nel 2003 una raccomandazione che mira a proteggere i consumatori contro le pratiche commerciali transfrontaliere fraudolente e ingannevoli<sup>32</sup>.

### 3.5.2. Azioni proposte

A livello multilaterale, alcuni Stati membri collaborano già attivamente in sedi internazionali (ad es. l'OCSE) nel cui ambito sono stati avviate attività anti-spam. Si incoraggia una partecipazione attiva a queste iniziative, in particolare ai fini della definizione di soluzioni a livello internazionale.

La Commissione accoglierà, nel febbraio 2004, un seminario dell'OCSE sullo spam finalizzato a migliorare la comprensione del problema e a contribuire all'elaborazione di soluzioni internazionali. Sulla base dei risultati del seminario l'OCSE avvierà successivamente azioni concrete di *follow-up*. I servizi della Commissione esaminano tali azioni di concerto con gli Stati membri, come pure le altre iniziative dell'OCSE in materia di promozione di una legislazione internazionale efficace, sensibilizzazione, soluzioni tecniche, autoregolamentazione e cooperazione internazionale nell'applicazione delle norme.

Per quanto riguarda le Nazioni Unite, la dichiarazione di principio del vertice mondiale sulla società dell'informazione (Ginevra, 10-12 dicembre 2003) ed il relativo piano d'azione sottolineano che lo spam è un problema che va affrontato agli adeguati livelli nazionali ed internazionali. La Commissione definirà le migliori modalità per garantire che nell'UE sia dato seguito ai risultati del vertice mondiale, in previsione del vertice di Tunisi che si terrà nel 2005.

Gli Stati membri e le autorità competenti sono anche invitati ad avviare o intensificare la cooperazione bilaterale con i paesi terzi. Ciò significa non solo promuovere l'adozione di una legislazione efficace ma anche cooperare ai fini dell'applicazione delle norme adottate, coinvolgendo, se necessario, anche le autorità di polizia e giudiziarie.

<sup>32</sup> “OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders”, OCSE, 2003.

Si incoraggia altresì la cooperazione tra autorità pubbliche e settore privato, in particolare ISP e ESP per risalire agli *spammer*, ferme restando le necessarie garanzie giuridiche.

I servizi della Commissione proseguiranno la loro attiva partecipazione ai lavori delle sedi internazionali, in particolare dell'OCSE, e collaboreranno all'organizzazione del seminario che la stessa Commissione accoglierà a Bruxelles nel febbraio 2004. Continueranno inoltre ad organizzare riunioni e contatti bilaterali con i paesi terzi per incoraggiare tali paesi ad adottare misure efficaci di lotta allo spam, in particolare nelle sue forme più offensive, e a promuovere la cooperazione in materia di applicazione delle norme.

I servizi della Commissione hanno iniziato ad esaminare, di concerto con gli Stati membri e le autorità nazionali interessate all'applicazione delle norme, le migliori modalità di cooperazione internazionale, in particolare per garantire il trattamento dei reclami relativi allo spam proveniente da paesi terzi. Questa collaborazione con le autorità nazionali proseguirà nel corso del 2004.

### **3.6. Monitoraggio**

#### *3.6.1. Discussione*

Per valutare il funzionamento pratico del sistema di consenso preliminare (“opt-in”) e ovviare efficacemente a determinati problemi, gli Stati membri dovranno disporre di informazioni oggettive e aggiornate sulle tendenze del fenomeno spam, dei reclami degli utenti e delle difficoltà incontrate dai prestatori di servizi. Le fonti ed il tipo di informazioni necessarie a tale scopo possono comprendere: tendenze sulla natura dei messaggi di spam, origine ed volume di e-mail commerciali indesiderate individuate da fornitori di software di filtraggio, prestatori di servizi e iniziative (di regolamentazione) nazionali e, se necessario, statistiche elaborate a partire dalle mailbox elettroniche messe a disposizione per i reclami.

Dal 2003 l'OCSE tenta di quantificare il volume di messaggi elettronici indesiderati a livello internazionale e proseguirà i suoi lavori nel 2004.

L'articolo 18 della direttiva sulla protezione della vita privata nel settore delle comunicazioni elettroniche stabilisce che entro il 2003 la Commissione pubblichi una relazione sull'applicazione della direttiva stessa e sull'impatto delle sue norme sugli operatori economici e sui consumatori, in particolare per quanto riguarda le disposizioni sulle comunicazioni indesiderate. Per elaborare questa relazione, la Commissione dovrà ottenere diverse informazioni, in particolare statistiche, dagli Stati membri.

#### *3.6.2. Azioni proposte*

Gli Stati membri devono disporre delle informazioni e delle statistiche necessarie per orientare i loro sforzi in materia di applicazione delle norme, se necessario in collaborazione con l'industria e tenendo conto delle attività dell'OCSE in materia di quantificazione del volume di messaggi elettronici indesiderati.

La Commissione si avvarrà dell'ausilio del nuovo gruppo informale online sulle comunicazioni commerciali indesiderate per facilitare e coordinare gli scambi di informazioni e di migliori pratiche sulle tendenze e le statistiche in materia di spam.

#### 4. AZIONI TECNICHE E AZIONI DI AUTOREGOLAMENTAZIONE DA PARTE DELL'INDUSTRIA

Il presente capitolo riguarda le misure proposte destinate principalmente agli operatori del mercato e si incentra su aspetti quali le disposizioni contrattuali, i codici di condotta, le pratiche commerciali accettabili, i marchi e le formule alternative di composizione delle controversie. Il capitolo descrive altresì alcune soluzioni tecniche, in particolare in materia di filtraggio e di protezione dei server.

##### 4.1. Applicazione efficace del regime “opt-in”

###### 4.1.1. *Discussione*

La lotta allo spam deve coinvolgere tutte le parti interessate. L'industria può svolgere un ruolo specifico in questo ambito facendo del regime “opt-in” una pratica commerciale ordinaria e quotidiana. Per pratica quotidiana si intende non solo l'applicazione di questo principio nei confronti degli utenti finali, ma anche alle transazioni con i partner commerciali.

In molti casi, occorre garantire un coordinamento più stretto attraverso le associazioni professionali ed una migliore partecipazione degli organismi settoriali di autoregolamentazione e delle associazioni di consumatori/utenti, nonché delle autorità per la protezione dati e di altre autorità nazionali competenti.

###### **Migliori pratiche**

Nei Paesi Bassi, ad esempio, la *Electronic Commerce Platform* ospita dal 2002 una piattaforma dedicata ai principi fondamentali delle comunicazioni elettroniche commerciali, che riunisce diversi esponenti del settore (imprese di marketing diretto e ISP) e l'associazione dei consumatori olandese. L'iniziativa si prefigge di garantire un'attuazione pratica del principio “opt-in”. Tale attuazione sarà sperimentata con l'autorità per la protezione dati<sup>33</sup>.

Anche i contratti possono risultare strumenti utili nella lotta allo spam, ferme restando le garanzie di tutela dei diritti individuali. Numerosi prestatori di servizi Internet (ISP) e prestatori di servizi di posta elettronica (ESP) inseriscono già nei contratti con i clienti disposizioni che vietano l'utilizzo dei loro servizi per l'invio di spam. Gli ISP e gli ESP proibiscono già l'invio di e-mail non richieste e l'invio indiscriminato di e-mail (detto anche *bulk e-mail*) dai loro *account* di posta elettronica<sup>34</sup>.

È molto probabile che i concetti utilizzati finora nei contratti stipulati tra gli ISP e i loro clienti siano diversi da quelli utilizzati nella nuova direttiva e nella legislazione nazionale di attuazione.

In termini di servizio alla clientela, occorre adottare un approccio più *proattivo* in materia di filtraggio informando in merito ai filtri anti-spam e proponendo agli abbonati di ricorrere a servizi o dispositivi di filtraggio in opzione.

<sup>33</sup> Cfr. <http://www.ecp.nl/projecten.php#32>

<sup>34</sup> Queste disposizioni sono talvolta dovute alla necessità di adottare tutte le misure necessarie per prevenire un uso inadeguato dei servizi. In altri casi, le disposizioni fanno riferimento a codici di condotta esistenti in materia di e-mail di massa (*bulk e-mail*) o a principi di autoregolamentazione (ad es. la cosiddetta *netiquette*).

Lo stesso principio si applica quando gli ISP e gli operatori di reti mobili stipulano contratti con terzi, in particolare con società di marketing diretto. Ciò riguarda non solo le relazioni dirette con le imprese che propongono servizi a “valore aggiunto”, ma anche gli accordi di interconnessione tra prestatori di servizi e operatori, come succede per i servizi mobili.

Il nuovo regime “opt-in” incide anche su molte attività di vendita diretta:

- i metodi utilizzati per la raccolta di indirizzi elettronici e di altre coordinate elettroniche devono essere conformi al nuovo regime (come indicato in precedenza, la raccolta di indirizzi elettronici è contraria al diritto comunitario);
- gli elenchi esistenti devono essere resi conformi;
- è vietato utilizzare dati senza il consenso degli interessati e vendere elenchi non conformi alla regolamentazione.

#### *4.1.2. Azioni proposte*

Occorre promuovere la partecipazione dell'industria e l'autoregolamentazione, o eventualmente la coregolamentazione, in particolare nei settori in cui la legislazione e il controllo dell'applicazione da parte delle pubbliche autorità rischiano di non essere sufficientemente efficaci. Tutte le parti interessate hanno un ruolo da svolgere in tale contesto, comprese le associazioni dei consumatori e/o degli utenti.

#### **Pratiche contrattuali dei prestatori di servizi nei confronti degli abbonati e dei partner commerciali**

In primo luogo, l'industria dovrà valutare la conformità dei contratti esistenti alle nuove disposizioni e procedere, se necessario, ai necessari adattamenti.

Si tratterà in particolare di adeguare le condizioni che figurano nei contratti di abbonamento. Vi sono tenuti non solo ISP e ESP, ma anche i prestatori di servizi mobili. A titolo complementare, gli operatori possono informare i clienti in merito ai filtri e ai software o servizi di filtraggio, e proporli in opzione come servizio alla clientela (in materia di filtraggio, cfr. anche punto 4.3). Anche le clausole dei contratti stipulati con i partner commerciali (ad es. interconnessione su reti mobili e servizi a valore aggiunto) devono vertere su pratiche commerciali conformi al regime “opt-in” e prevedere sanzioni adeguate in caso d'infrazione.

#### **Pratiche delle società di vendita diretta**

In secondo luogo, le società di vendita diretta potrebbero essere tenute ad adattare le loro pratiche al regime “opt-in” e, in particolare, concordare metodi specifici e leciti di raccolta dei dati personali (“opt-in” doppio o confermato).

#### **Codici di condotta**

In terzo luogo, le associazioni settoriali hanno già annunciato diverse iniziative (adattamento o adozione di codici di condotta e diffusione di buone pratiche

commerciali<sup>35</sup>). La Commissione sosterrà l'elaborazione di codici di condotta online su scala europea nel settore della vendita diretta. I codici di condotta, le altre iniziative di autoregolamentazione e i contratti devono essere conformi al regime “opt-in”. Il coinvolgimento della competente autorità di regolamentazione potrebbe essere utile a tale riguardo. Occorre ricordare che il gruppo di lavoro “Articolo 29 - protezione dati” può approvare codici di condotta elaborati a livello comunitario (cfr. articolo 30 della direttiva 95/46/CE, ossia la direttiva “generale” in materia di protezione dati).

L'effettiva applicazione delle soluzioni basate sull'autoregolamentazione dipende dalla struttura che sarà costituita per controllare la conformità alle norme concordate, e in particolare l'efficacia delle sanzioni previste.

## **Marchi**

In quarto luogo, per sensibilizzare ulteriormente gli utenti si potrebbe ricorrere a strumenti quali i marchi (noti come marchi di fiducia o *webseals*), in particolare quando il rispetto dei codici di condotta da parte degli operatori del mercato è verificato e certificato da terze parti di fiducia.

La presenza di marchi visibili può aiutare gli utenti a individuare gli ISP, gli ESP e gli altri operatori che si conformano alle norme UE e/o a codici di condotta riconosciuti che danno attuazione a tali norme. I marchi possono inoltre contribuire a rafforzare l'efficacia dei sistemi di filtraggio.

Tali marchi potrebbero altresì essere apposti ai database di utenti e ai messaggi elettronici conformi al regime “opt-in” (ad esempio, apposizione del marchio ADV - per “advertising” - nella rubrica “oggetto” di una e-mail per segnalare che contiene pubblicità).

Grazie a tali marchi i destinatari possono identificare chiaramente le comunicazioni commerciali conformemente alla direttiva sul commercio elettronico (cfr. articolo 6, lettera a) della direttiva 2000/31/CE e punto 2 qui sopra).

## **4.2. Meccanismi alternativi di composizione delle controversie**

### *4.2.1. Discussione*

In caso di violazione della privacy, come nel caso di invio di una comunicazione commerciale indesiderata, il ricorso ad un meccanismo di composizione extragiudiziale garantirebbe maggiore conformità alle nuove norme. Sono state lanciate varie iniziative a livello nazionale e comunitario per creare meccanismi alternativi di composizione delle controversie in materia di transazioni e comunicazioni elettroniche. Nel 1998 e nel 2001 la Commissione ha adottato due raccomandazioni in materia di meccanismi alternativi di composizione in cui stabilisce i principi applicabili a tali regimi. Sono in corso numerose iniziative relative a meccanismi alternativi di composizione per le materie attinenti alla tutela dei consumatori (ad es. la rete extragiudiziale europea EEJ-NET)<sup>36</sup>. Anche

---

<sup>35</sup> La Federazione europea di marketing diretto (FEDMA) ha annunciato la pubblicazione online di un codice di condotta destinato alle società che operano in questo settore.

<sup>36</sup> Per ulteriori informazioni cfr.:  
[http://europa.eu.int/comm/consumers/redress/out\\_of\\_court/index\\_en.htm](http://europa.eu.int/comm/consumers/redress/out_of_court/index_en.htm)

l'articolo 17 della direttiva sul commercio elettronico incoraggia lo sviluppo di meccanismi di questo tipo.

Taluni paesi dispongono di meccanismi di composizione extragiudiziale. Talvolta previsti per legge, tali meccanismi differiscono gli uni dagli altri sotto diversi aspetti quali l'origine (meccanismi settoriali: applicabili alla vendita diretta o alla vendita per posta elettronica), la "giurisdizione", le competenze e le sanzioni (ad es. risarcimento danni), la partecipazione di determinate autorità (ad es. le autorità per la protezione dati, gli organismi di etica pubblicitaria) ecc.

L'efficacia di questi meccanismi dipende da una serie di condizioni che riguardano in particolare la loro organizzazione e la loro promozione, nonché le misure adottate per garantire l'applicazione delle loro decisioni. L'istituzione di tali meccanismi presuppone inoltre una cooperazione tra autorità pubblica e industria.

#### 4.2.2. *Azioni proposte*

Si incoraggia l'istituzione di efficaci meccanismi di reclamo fondati sull'autoregolamentazione e di meccanismi alternativi di composizione delle controversie basati, nella misura del possibile, su iniziative esistenti (ad es. la rete EEJ-NET). Tali meccanismi potrebbero risultare particolarmente utili nei casi in cui è difficile ottenere una cooperazione internazionale.

### 4.3. **Questioni tecniche**

#### 4.3.1. *Discussione*

Vengono utilizzati diversi mezzi tecnici per contrastare lo spam. La stessa comunità Internet (RIPE, IETF ecc.) affronta con la massima serietà il problema<sup>37</sup>. Il presente documento non esamina le soluzioni a più lungo termine come le nuove norme tecniche applicabili alla posta elettronica. Gli ISP e gli ESP bloccano spesso i messaggi che provengono da server utilizzati per l'invio di spam (lista nera) finché la fonte dello spam non viene identificata e le viene negato l'uso del server. Inoltre, gli utenti possono installare software di filtraggio sui loro terminali e i prestatori di servizi di comunicazione elettronica ne possono dotare i loro server.

Non tutte le tecniche di filtraggio permettono lo stesso livello di controllo da parte dell'utente né offrono le stesse garanzie in termini di protezione dei dati e della privacy, in particolare della riservatezza delle comunicazioni. Potrebbero inoltre non essere ancora conformi al nuovo regime "opt-in" applicabile nei paesi dell'UE in materia di comunicazioni commerciali (consenso preliminare, attività di prospezione commerciale, e-mail indiscriminate e personalizzate). Del resto, una più chiara distinzione tra le attività di marketing lecite (pratiche conformi al regime "opt-in") e le comunicazioni commerciali indesiderate faciliterebbe lo sviluppo di software di filtraggio più efficaci.

---

<sup>37</sup> Ad esempio il gruppo di lavoro anti-spam del RIPE (reti IP europee) è attivo sin dal 1998 (cfr. il documento "*Good Practice for combating Unsolicited Bulk Email*" pubblicato sul sito RIPE (<http://www.ripe.net>). Più di recente la *Internet Research Task Force* (IRTF) ha istituito un gruppo di ricerca sulla lotta anti-spam (cfr.: <http://www.irtf.org/charters/asrg.html>). Questo gruppo potrebbe elaborare alcune tecnologie che fungerebbero da punto di partenza per le attività di normalizzazione avviate nell'ambito dell'*Internet Engineering Task Force* (IETF).

Se, da un lato, le nuove disposizioni giuridiche sulla posta elettronica commerciale indesiderata prevedono garanzie supplementari per l'utente e offrono ai prestatori di servizi maggiore certezza del diritto per perseguire, su richiesta, gli *spammer*, dall'altro, può succedere che i dispositivi di filtraggio blocchino messaggi leciti (“falsi positivi”) o lascino passare messaggi di spam (“falsi negativi”). In alcuni casi, si rischia che il mittente o il destinatario reale intraprenda un'azione giudiziaria nei confronti di un ISP/ESP. Taluni ISP/ESP propongono pertanto il servizio di filtraggio come opzione commerciale e chiedono all'utente l'autorizzazione di attivarlo.

Seppure tali aspetti esulino dal campo di applicazione della presente comunicazione, va osservato che il ricorso a tecniche di filtraggio pone una serie di problemi di altro tipo quali la relazione tra filtraggio e libertà di espressione e tra filtraggio e obbligo contrattuale di ISP/ESP di trasmettere messaggi di posta elettronica ai clienti dei loro clienti.

Per quanto riguarda i servizi mobili, dato che i modelli commerciali sono diversi da quelli dei servizi Internet fissi, possono essere adottate soluzioni di filtraggio diverse. Nel caso dei servizi mobili, il fatto che tradizionalmente venga fatturato ogni messaggio consegnato rende lo spam più costoso. Tuttavia, per alcuni nuovi servizi la fatturazione è basata sul recupero del messaggio, il che significa che lo spam comporta costi supplementari per il destinatario. Inoltre, messaggi di posta elettronica possono ormai essere ricevuti su terminali mobili. Gli abbonati dovrebbero quindi disporre di filtri e funzioni di visualizzazione che consentano loro di gestire lo “spam mobile”.

Particolare attenzione meritano anche i cosiddetti “relay aperti”. Per relay aperti si intendono i server SMTP che possono essere utilizzati per trasmettere messaggi inviati da utenti che non sono utenti locali del server. In passato, la maggior parte dei relay erano aperti. Questi, tuttavia, possono essere facilmente utilizzati dagli *spammer* per inviare comunicazioni indesiderate. Semplici misure preventive consentirebbero di ridurre le pratiche abusive in questo settore. Le stesse osservazioni valgono per i proxy aperti, ossia i server che utilizzano software che permettono un'interazione diretta con Internet.

#### 4.3.2. Azioni proposte

Gli Stati membri e le autorità competenti sono invitati a precisare le condizioni giuridiche che disciplinano il funzionamento dei vari tipi di software di filtraggio nei rispettivi paesi, anche dal punto di vista del rispetto della privacy.

I fornitori di software di filtraggio devono fare in modo che i loro sistemi siano compatibili con il regime “opt-in” e con gli altri requisiti del diritto comunitario, compresi quelli relativi alla riservatezza delle comunicazioni.

Gli utenti devono poter gestire lo spam in arrivo secondo le loro necessità. I fornitori di software di filtraggio devono tenere conto delle conseguenze, per gli utenti, dei “falsi positivi”, dei “falsi negativi”, di alcune forme di filtraggio basate sui contenuti e dei problemi di responsabilità che potrebbero risultarne.

I fornitori di software di filtraggio devono collaborare con le parti interessate per sviluppare tecniche di riconoscimento delle e-mail corrispondenti alle pratiche commerciali conformi al diritto comunitario (marchi di fiducia, *webseals* ecc.).

I prestatori di servizi di posta elettronica (e eventualmente di servizi mobili) devono proporre in opzione dispositivi/servizi di filtraggio ai clienti che ne fanno richiesta, ed informarli su quelli proposti da terzi.

I proprietari di server di posta elettronica devono provvedere ad un'adeguata protezione dei loro server e far sì che questi non funzionino in modalità "relay aperto" (salvo se necessario). La stessa raccomandazione vale per i server proxy aperti.

## 5. AZIONI DI SENSIBILIZZAZIONE

Questo capitolo verte sulle azioni proposte in materia di prevenzione, sensibilizzazione dei consumatori e segnalazione dei problemi.

### 5.1. Discussione

Gli Stati membri erano tenuti a recepire il nuovo regime "opt-in" in materia di messaggi di posta elettronica indesiderati nel diritto interno entro il 31 ottobre 2003. Malgrado questo nuovo approccio abbia beneficiato di un ampio riscontro nella stampa, sussiste incertezza, tra operatori del mercato e grande pubblico, su cosa significhi in pratica il regime "opt-in"<sup>38</sup>.

Il nuovo approccio si basa sul principio che all'utente è riconosciuto il diritto di accettare o rifiutare di ricevere comunicazioni commerciali. Ciò implica tuttavia che l'utente conosca le norme di base applicabili alle comunicazioni indesiderate e sappia dove segnalare eventuali violazioni.

#### Migliori pratiche

L'*Information Commission* (autorità per protezione dati nel Regno Unito) ha pubblicato, qualche settimana prima dell'entrata in vigore della nuova regolamentazione che dà attuazione alla direttiva, un documento di orientamento per spiegare le nuove norme applicabili, di cui una parte era dedicata alla vendita con mezzi elettronici. L'autorità ha inoltre annunciato che, al momento dell'entrata in vigore delle nuove norme, formulari di reclamo contenenti tutte le informazioni necessarie saranno disponibili online e presso gli uffici dell'autorità stessa<sup>39</sup>.

Gli utenti devono essere consapevoli dei rischi legati alla comunicazione dei propri dati personali via Internet (ad esempio sui siti web o i forum Usenet visitati) e adattare il loro comportamento di conseguenza.

Devono infine essere informati dei tipi di software di filtraggio disponibili in commercio e dell'assistenza che possono ricevere da prestatori di servizi (ad es. ISP e ESP) e fornitori di software.

---

<sup>38</sup> Informazioni di riferimento sulle norme applicabili alle comunicazioni indesiderate ai sensi della direttiva 2002/58/CE possono essere ottenute al seguente indirizzo:  
[http://europa.eu.int/information\\_society/topics/ecom/all\\_about/todays\\_framework/privacy\\_protection/index\\_en.htm#unsolicited](http://europa.eu.int/information_society/topics/ecom/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited)

<sup>39</sup> Cfr.:  
[http://www.dti.gov.uk/industries/ecomunications/directive\\_on\\_privacy\\_electronic\\_communications\\_200258ec.html#guidance](http://www.dti.gov.uk/industries/ecomunications/directive_on_privacy_electronic_communications_200258ec.html#guidance)

## Migliori pratiche

La *Commission Nationale Informatique et Libertés* (CNIL, autorità francese per la protezione dati) ha pubblicato sul proprio sito un dossier informativo molto completo riguardante vari aspetti dello spam (risultati della campagna “*boîte à spam*”, casi deferiti alle autorità giudiziarie (cfr. infra), consigli di prevenzione, informazioni sul modo di segnalare lo spam, estremi delle associazioni di utenti che operano in questo settore ecc.).

Benché la maggior parte degli Stati membri abbia avviato o preveda di avviare attività di sensibilizzazione sul nuovo regime “opt-in”, tali iniziative sono estremamente diverse tra loro in termini di calendario di realizzazione, natura delle informazioni fornite, pubblico target e partecipanti. Alcuni Stati membri tuttavia hanno preferito aspettare fino all’entrata in vigore della nuova legislazione. Le consultazioni pubbliche organizzate in merito all’attuazione della direttiva 2002/58/CE hanno sempre contribuito, in una certa misura, alla sensibilizzazione del pubblico.

A seconda degli Stati membri e delle diverse attribuzioni a livello nazionale queste attività possono essere di competenza di vari organismi (autorità per la protezione dati, ANR, autorità per la tutela dei consumatori, mediatori/ombudsman). Non tutti gli Stati membri garantiscono (al momento) un coordinamento tra le varie autorità competenti. In alcuni Stati membri i ministeri partecipano al processo. È frequente la partecipazione di associazioni settoriali. A volte sono coinvolte anche le associazioni di consumatori o di utenti.

Alcuni esponenti dell’industria hanno avviato attività di sensibilizzazione su scala nazionale, comunitaria o mondiale, ma anche in questo caso le iniziative possono variare in modo notevole. Le attività comprendono in particolare:

- guide pratiche destinate alle società di vendita diretta o campagne di informazione destinate settore della comunicazione;
- orientamenti generali alla clientela in merito ai codici di condotta, ai meccanismi di reclamo e ai sistemi di filtraggio;
- piattaforme/gruppi di lavoro incaricati di elaborare buone pratiche per le comunicazioni commerciali.

## 5.2. Azioni proposte

Per capire meglio cosa sia autorizzato e cosa sia vietato fare in materia di e-mail commerciali, è necessario avviare rapidamente in tutti gli Stati membri un’azione durevole e di ampia portata, sia nel campo della prevenzione che dell’applicazione delle norme. Occorre fornire informazioni pratiche sulla prevenzione, le pratiche di marketing lecite e le soluzioni tecniche e giuridiche a disposizione degli utenti.

Tutte le parti sono invitate a svolgere il proprio ruolo nelle attività di sensibilizzazione, dagli Stati membri alle autorità competenti, fino alle

### Il programma Safer Internet e lo spam

La Commissione europea ha pubblicato un invito per il programma “Safer Internet” nell’ambito delle cui linee di azione (ad es. sensibilizzazione) possono essere proposti progetti destinati a trattare la problematica dello spam. I progetti selezionati a seguito del primo esercizio di valutazione potrebbero essere avviati nel maggio 2004.

La Commissione prepara attualmente la proposta relativa alla prosecuzione del programma – “Safer Internet plus” – in cui si prevede di finanziare nuove misure di contrasto ai contenuti illegali e nocivi e ai contenuti indesiderati come lo spam.

[http://www.europa.eu.int/information\\_society/programmes/iap/call/index\\_en.htm](http://www.europa.eu.int/information_society/programmes/iap/call/index_en.htm)

associazioni di consumatori/utenti e alle imprese. Gli Stati membri e le autorità competenti che non hanno ancora fatto il necessario sono invitati a lanciare o sostenere campagne di sensibilizzazione all'inizio del 2004.

Per quanto riguarda in particolare la natura delle informazioni fornite, le attività di sensibilizzazione destinate alle imprese e/o ai consumatori devono comprendere i seguenti elementi:

- spiegazioni di base, ma ampiamente diffuse, sulle nuove norme e sui diritti che ne derivano per le imprese e/o i consumatori;
- informazioni pratiche sulle prassi di commercializzazione accettabili ai sensi del regime “opt-in”, che spieghino in particolare quando la raccolta di dati personali è lecita;
- informazioni pratiche sul modo in cui i consumatori possono evitare lo spam (ad es. uso dei dati personali ecc.);
- informazioni pratiche destinate ai consumatori sui prodotti e i servizi anti-spam disponibili (ad es. filtraggio, protezione);
- informazioni sulle misure pratiche da adottare in caso di spam, in particolare sui meccanismi di reclamo e su eventuali meccanismi alternativi di composizione delle controversie.

Le suddette azioni devono essere dirette alle seguenti categorie target:

- a) imprese che operano nel campo della vendita diretta o fanno ricorso a tali tecniche;
- b) abbonati ai servizi di posta elettronica, compresi i servizi SMS;
- c) prestatori di servizi di posta elettronica, compresi i prestatori di servizi mobili.

Le attività di sensibilizzazione devono esplicarsi attraverso diversi canali (e non solo sul web) al fine di raggiungere efficacemente i vari gruppi target. È importante, a tal fine, la partecipazione dell'industria e delle associazioni dei consumatori. Occorre infine garantire il coordinamento tra le varie iniziative possibili.

Le azioni sopraelencate devono vertere anche sui codici di condotta settoriali efficaci, sui meccanismi di reclamo, sui marchi (ad es. marchi di fiducia) e, laddove possibile, sui sistemi di certificazione.

I servizi della Commissione forniscono già informazioni sui principi di base del regime “opt-in” sul sito web EUROPA<sup>40</sup>. Grazie a *link* ipertestuali il sito rinvierà inoltre agli aspetti nazionali dell'attuazione, alle statistiche essenziali e alle tendenze del fenomeno

---

<sup>40</sup>

Cfr:

[http://europa.eu.int/information\\_society/topics/ecom/highlights/current\\_spotlights/spam/index\\_en.htm](http://europa.eu.int/information_society/topics/ecom/highlights/current_spotlights/spam/index_en.htm)

[http://europa.eu.int/information\\_society/topics/ecom/all\\_about/todays\\_framework/privacy\\_protection/index\\_en.htm#unsolicited](http://europa.eu.int/information_society/topics/ecom/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited)

spam. I servizi della Commissione ricorreranno inoltre alla collaborazione degli Eurosportelli per diffondere informazioni sulle nuove norme.

## CONCLUSIONI

Lo spam è una delle principali sfide alle quali deve far fronte Internet. Per lottare contro questo fenomeno, tuttavia, occorrerà intervenire su vari fronti; sarà necessario agire efficacemente non solo sul piano dell'applicazione delle norme e della cooperazione internazionale, ma anche convincere l'industria ad adottare soluzioni di autoregolamentazione e soluzioni tecniche, nonché sensibilizzare i consumatori. Il prospetto riportato nelle pagine seguenti contiene una sintesi delle azioni individuate nella presente comunicazione.

La Commissione sosterrà ovviamente questi sforzi per quanto possibile, ma saranno soprattutto gli Stati membri e le loro autorità competenti, l'industria, i consumatori e gli utenti di Internet e dei servizi di comunicazione elettronica a dover svolgere un ruolo attivo, sia a livello nazionale che internazionale.

L'attuazione integrata e parallela delle tipologie di azioni individuate nella presente comunicazione, che beneficia di un ampio sostegno delle parti interessate, può contribuire ad arginare sensibilmente lo spam, il cui volume rischia attualmente di vanificare i vantaggi dell'e-mail e degli altri mezzi di comunicazione elettronica per la società e le economie dei nostri paesi.

La Commissione seguirà da vicino l'attuazione di queste azioni nel 2004, in particolare mediante il gruppo informale per le comunicazioni indesiderate e valuterà, al più tardi per la fine del 2004, la necessità di eventuali azioni supplementari o correttive.

## TABELLA DELLE AZIONI INDIVIDUATE NELLA COMUNICAZIONE

Nella tabella qui sotto sono riassunte le azioni individuate nella comunicazione. Le azioni che dipendono dalla Commissione e dai servizi della Commissione sono state elencate separatamente. Come indicato in precedenza, le azioni sono intercorrelate in diversi modi e devono essere attuate nella misura del possibile in modo parallelo ed integrato.

### **I - Attuazione ed applicazione efficaci da parte degli Stati membri e delle autorità competenti**

La condizione preliminare è che gli Stati membri provvedano senza ulteriori ritardi al recepimento della direttiva sulla tutela della vita privata nel settore delle comunicazioni elettroniche, e in particolare delle disposizioni relative alle comunicazioni indesiderate.

Gli Stati membri e le autorità competenti devono valutare l'efficacia dei loro meccanismi di applicazione (ricorsi e sanzioni, meccanismi di reclamo, cooperazione tra gli Stati membri e cooperazione con i paesi terzi, monitoraggio). Essi devono inoltre definire strategie nazionali che garantiscano la cooperazione tra le autorità per la protezione dati, le autorità per la tutela dei consumatori e le ANR, ed evitino sovrapposizioni e duplicazioni di competenze tra i vari organismi.

Gli Stati membri e le autorità competenti devono in particolare vigilare ai seguenti aspetti:

#### **a) Ricorsi e sanzioni efficaci:**

- garantire alle vittime adeguate possibilità di richiedere un risarcimento e prevedere sanzioni effettive, anche pecuniarie, e, se necessario, penali;
- gli Stati membri che non dispongono di vie di ricorso amministrativo devono dotarsi di questi strumenti per garantire un'adeguata applicazione delle nuove norme;
- dotare le autorità competenti dei necessari poteri investigativi ed esecutivi.

#### **b) Meccanismi di reclamo:**

- stabilire meccanismi di reclamo adeguati, in particolare mailbox elettroniche destinate a ricevere i reclami degli utenti;
- coordinare l'azione delle varie autorità nazionali competenti.

#### **c) Reclami transfrontalieri e cooperazione in materia di controllo dell'applicazione all'interno dell'UE:**

- utilizzare un meccanismo di collegamento esistente (o crearne uno nuovo) per permettere alle autorità nazionali di cooperare in materia di applicazione delle norme a livello transfrontaliero all'interno dell'UE (scambio di informazioni, mutua assistenza). In tale contesto, per quanto riguarda in particolare lo spam fraudolento e ingannevole, il Consiglio ed il Parlamento sono invitati a giungere quanto prima ad un accordo in merito alla proposta di regolamento relativo alla cooperazione in materia di tutela dei consumatori e ad esaminare l'opportunità di estenderne il campo di applicazione alla direttiva sulla tutela della vita privata nel settore delle comunicazioni elettroniche.

#### **d) Cooperazione con i paesi terzi:**

- partecipare attivamente ai lavori delle sedi multilaterali (ad esempio l'OCSE) per elaborare soluzioni a livello internazionale;

- rafforzare o avviare una cooperazione bilaterale con i paesi terzi;
- esaminare con la Commissione quali iniziative specifiche questa potrebbe avviare a sostegno della cooperazione internazionale;
- cooperare con il settore privato per individuare gli *spammer*, ferme restando le adeguate garanzie giuridiche.

**(e) Monitoraggio:**

- provvedere ad acquisire le informazioni e i dati statistici necessari per valutare i propri sforzi in materia di applicazione delle norme, se necessario in cooperazione con l'industria e tenendo conto delle attività in materia di quantificazione dello spam in corso presso l'OCSE.

## **II – Azioni di autoregolamentazione e azioni tecniche da parte dell'industria**

Gli operatori del mercato (ISP, ESP, operatori di reti mobili, società di sviluppo di software, società di vendita diretta) devono fare del regime “opt-in” una pratica ordinaria, se necessario in cooperazione con le associazioni di consumatori e di utenti e le autorità competenti, e avviare in particolare le seguenti azioni:

### **a) Azioni di autoregolamentazione:**

- valutare e, se necessario, adattare le pratiche contrattuali dei prestatori di servizi (ISP, ESP, operatori di reti mobili) nei confronti degli abbonati e dei partner commerciali; informare sul filtraggio ed eventualmente offrire software o servizi di filtraggio come servizio in opzione ai clienti;

- adeguare le pratiche di vendita diretta al regime “opt-in” ed eventualmente concordare metodi di raccolta dei dati personali specifici e conformi alla legislazione (ad es. sistema “opt-in” doppio o confermato);

- elaborare e diffondere codici di condotta efficaci (ad es. iniziativa FEDMA) conformi al regime “opt-in”, in cooperazione, se necessario, con il gruppo di lavoro “articolo 29 - protezione dati” o con le autorità nazionali competenti;

- prevedere l'uso di marchi per le e-mail e i database conformi al regime “opt-in” per aiutare gli utenti (e i sistemi di filtraggio) a riconoscerli, conformemente alla direttiva sul commercio elettronico;

- utilizzare o, se necessario, istituire, nel quadro dell'autoregolamentazione, meccanismi di reclamo e formule alternative di composizione delle controversie che siano efficaci e si basino nella misura del possibile su iniziative esistenti (ad es. rete EEJ-NET).

### **b) Azioni tecniche:**

- (i fornitori di software di filtraggio) devono fare in modo che i loro sistemi siano conformi al regime “opt-in” e alle altre esigenze del diritto comunitario, anche in materia di riservatezza delle comunicazioni. Gli Stati membri e le autorità competenti sono invitati a chiarire le condizioni giuridiche che disciplinano il funzionamento dei vari tipi di software di filtraggio nei loro paesi, anche dal punto di vista del rispetto della privacy;

- (i fornitori di software di filtraggio) devono tenere conto delle conseguenze, per gli utenti, dei casi di “falso positivo”, di “falso negativo” e di alcune forme di filtraggio basate sui contenuti, nonché dei problemi di responsabilità che potrebbero derivarne. Gli utenti devono poter gestire lo spam in entrata in funzione delle loro necessità;

- (i fornitori di software di filtraggio) devono collaborare con le parti interessate per sviluppare tecniche di riconoscimento delle e-mail commerciali lecite (ossia conformi alle pratiche commerciali accettate ai sensi del diritto comunitario), utilizzando ad esempio appositi marchi;

- (i prestatori di servizi di posta elettronica e, eventualmente, di servizi mobili) devono offrire in opzione dispositivi o servizi di filtraggio ai clienti che ne fanno richiesta, e informarli su quelli proposti da terzi;

- (i proprietari di server di posta elettronica) devono assicurarsi che i loro server siano correttamente protetti e non si trovino in modalità “relay aperto”, salvo se necessario. La stessa osservazione vale per i server proxy aperti.

### **III – Azioni di sensibilizzazione da parte degli Stati membri, dell'industria e delle associazioni di consumatori/utenti**

Gli Stati membri e le autorità competenti che non hanno ancora fatto il necessario sono invitati a lanciare o sostenere campagne di sensibilizzazione all'inizio del 2004.

Tutte le parti interessate (Stati membri e autorità competenti, associazioni di consumatori e/o di utenti, industria) devono partecipare attivamente alle campagne di informazione pratica in materia di prevenzione, pratiche di vendita accettabili e soluzioni tecniche e giuridiche destinate agli utenti, e in particolare:

- orientare le loro azioni verso: a) le imprese di vendita diretta e le imprese che fanno ricorso a queste tecniche; b) gli abbonati a servizi di posta elettronica, compresi i servizi SMS e c) i prestatori di servizi di posta elettronica, compresi i prestatori di servizi mobili;
- fornire alle imprese e/o ai consumatori:
- spiegazioni di base, ma ampiamente diffuse, sulle nuove norme e sui diritti che ne derivano;
- informazioni pratiche sulle prassi commerciali accettabili ai sensi del regime “opt-in” e spiegazioni circa la legittimità della raccolta di dati personali;
- informazioni pratiche sul modo in cui i consumatori possono evitare lo spam (ad es. uso dei dati personali ecc.);
- informazioni pratiche destinate ai consumatori sui prodotti e i servizi anti-spam disponibili (ad es. filtraggio, protezione);
- informazioni sulle misure pratiche da adottare in caso di spam, in particolare sui meccanismi di reclamo e su eventuali meccanismi alternativi di composizione delle controversie;
- informare in merito ai codici di condotta efficaci dell'industria, ai meccanismi di reclamo, ai marchi (ad es. marchi di fiducia) e a eventuali sistemi di certificazione;
- condurre le attività di sensibilizzazione ricorrendo a canali diversi, sia online che offline, al fine di raggiungere le varie categorie di pubblico target.

A tal fine è indispensabile provvedere al coinvolgimento dell'industria e delle associazioni dei consumatori. Occorre inoltre garantire il coordinamento delle varie iniziative.

#### **IV – Azioni di competenza della Commissione e dei suoi servizi**

La Commissione sorveglierà l'attuazione delle azioni sopra descritte nel corso del 2004, in particolare mediante il gruppo informale sulle comunicazioni indesiderate, e valuterà entro la fine del 2004 la necessità di eventuali azioni supplementari o correttive.

In linea generale, la Commissione continuerà a sorvegliare attentamente la messa in applicazione della direttiva, verificando in particolare se le disposizioni nazionali di attuazione prevedono sanzioni effettive, anche finanziarie o penali, in caso di violazione delle sue disposizioni. (La Commissione ha avviato nel novembre 2003 procedimenti di infrazione nei confronti di diversi Stati membri per mancata notifica delle misure nazionali di attuazione.) Se necessario, i servizi della Commissione sono pronti ad assistere gli Stati membri in questo compito.

I servizi della Commissione hanno istituito, con l'assistenza degli Stati membri e delle autorità per la protezione dati, un gruppo informale online sulle comunicazioni commerciali indesiderate, incaricato di collaborare alle attività legate all'effettiva applicazione della direttiva (ad es. in materia di reclami, ricorsi, sanzioni, cooperazione internazionale) e alle altre azioni individuate nella presente comunicazione.

I servizi della Commissione chiederanno al gruppo di lavoro "articolo 29 - protezione dati" di adottare al più presto un parere su alcuni concetti della direttiva sulla tutela della vita privata nel settore delle comunicazioni elettroniche al fine di contribuire ad un'applicazione uniforme delle misure nazionali adottate ai sensi della direttiva.

I servizi della Commissione hanno cominciato ad esplorare, di concerto con gli Stati membri e con le autorità nazionali interessate all'applicazione della direttiva, i migliori mezzi per garantire un'applicazione transfrontaliera delle norme nell'UE e nei paesi terzi. Questa collaborazione con le autorità nazionali proseguirà nel 2004.

La Commissione sosterrà la definizione di codici di condotta online europei per la vendita diretta, sottoponendoli se necessario all'approvazione del gruppo di lavoro "articolo 29 - protezione dati".

La Commissione accoglierà, nel febbraio 2004, un seminario OCSE dedicato allo spam ed esaminerà con gli Stati membri le necessarie azioni per darvi seguito, compresi i lavori dell'OCSE in materia di promozione di una legislazione efficace a livello internazionale, sensibilizzazione, soluzioni tecniche, autoregolamentazione e cooperazione internazionale per l'applicazione delle norme.

La Commissione definirà inoltre come dar seguito, nell'UE, ai risultati del vertice mondiale del 2003 sulla società dell'informazione, in previsione del vertice di Tunisi che si terrà nel 2005.

La Commissione ha pubblicato un invito a presentare proposte per il programma "Safer Internet", le cui diverse azioni permettono di proporre progetti di lotta allo spam; la Commissione prepara attualmente una proposta di prosecuzione del programma (proposta "Safer Internet *Plus*") che prevede il finanziamento di misure supplementari, in particolare di lotta anti-spam.

I servizi della Commissione continueranno a fornire informazioni sui principi di base del regime "opt-in" sul sito web EUROPA. Grazie a *link* ipertestuali il sito rinvierà inoltre agli aspetti nazionali dell'attuazione, alle statistiche essenziali e alle tendenze del fenomeno spam. I servizi della Commissione ricorreranno inoltre alla collaborazione degli Eurosportelli per diffondere informazioni sulle nuove norme.