



DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY  
COMMITTEE ON CONSUMER POLICY  
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

## **Task Force on Spam**

### **MISURE E POLITICHE RACCOMANDATE CONTRO LO SPAM: EXECUTIVE SUMMARY**

(DSTI/CP/ICCP/SPAM(2005)3/FINAL)

Traduzione (non-ufficiale) in italiano del documento dell'OECD "Anti-spam toolkit of recommended policies and measures: executive summary". Si ringrazia il [Ministero per l'Innovazione e le Tecnologie](#) italiano per la traduzione del presente documento.

*Italian translation (unofficial) of the OECD Anti-Spam Toolkit Executive Summary. We wish to thank the Italian Minister of Innovation and Technologies for the translation of this document.*

## INDICE

Prefazione .....	3
Nascita ed evoluzione dello spam.....	4
Un approccio coerente e coordinato allo spam .....	4
Elemento I. Approcci regolamentari.....	6
Elemento II. Applicazione della normativa .....	9
RACCOMANDAZIONE DEL CONSIGLIO SULLA COOPERAZIONE TRANSFRONTALIERA IN MATERIA DI APPLICAZIONE DELLE NORMATIVE CONTRO LO SPAM .....	11
Elemento III. Iniziative di settore .....	14
Elemento IV. Soluzioni tecniche .....	16
Elemento V. Iniziative di educazione e sensibilizzazione degli utenti .....	16
Elemento VI. Partnership pubblico/privato .....	18
Elemento VII. Metriche .....	18
Elemento VIII. Cooperazione globale .....	18

## **Prefazione**

Il presente documento offre una sintesi dell'Antispam Toolkit Report dell'OCSE (il Rapporto) e comprende le politiche e misure raccomandate dal Rapporto oltre che la Raccomandazione del Consiglio dell'OCSE sulla cooperazione transnazionale in materia di applicazione delle normative antispam.

Il Toolkit completo è pubblicato in formato cartaceo, ma è disponibile anche in formato elettronico all'indirizzo [www.oecd-antispam.org](http://www.oecd-antispam.org) e comprende il Rapporto della Task Force, diviso nei suoi otto elementi principali, le migliori pratiche BIAC e MAAWG sugli ISP e gli operatori di rete e le migliori pratiche BIAC sul marketing via e-mail. Sono inoltre disponibili delle linee guida per la collaborazione fra autorità (Spam Referral proforma) elaborate da CNSA/LAP, e un codice di buone pratiche degli operatori di telefonia mobile contro lo spam (Mobile Spam Code of Practice), elaborato dalla GSM Association.

## ANTISPAM TOOLKIT: MISURE E POLITICHE RACCOMANDATE EXECUTIVE SUMMARY\*

Considerati la diffusione dello spam e il rischio di ulteriori problemi risultanti dalla convergenza delle tecnologie di comunicazione e dall'emergenza di strumenti di comunicazione ubiqui e portatili e dell'Internet mobile, l'OCSE ha creato una **Task Force contro lo spam** (di seguito "Task Force") composta da responsabili politici ed esperti di settore, cui è affidato il compito di sviluppare un quadro di riferimento per affrontare il problema dello spam mediante un'ampia gamma di soluzioni multidisciplinari.

La Task Force ha elaborato un **kit di strumenti antispam** ("toolkit"), in cui raccomanda una gamma di politiche e misure per la formulazione di un assetto di politiche pubbliche di ampio respiro atto ad affrontare il problema dello spam. Tali politiche e misure sono riassunte qui di seguito.

### **Nascita ed evoluzione dello spam**

Affidabilità, efficienza e fiducia sono caratteristiche necessarie affinché le piattaforme elettroniche, i programmi applicativi e i servizi di comunicazione elettronica possano contribuire allo sviluppo economico e sociale. Oggi, tuttavia, il funzionamento dell'e-mail e di altri strumenti di comunicazione elettronica è minacciato dalla diffusione di messaggi non richiesti, indesiderati e dannosi, un fenomeno comunemente noto come spam. Se non opportunamente arginate, queste minacce rischiano di logorare la fiducia degli utenti.

Il fenomeno dello spam, nato con l'invio di messaggi elettronici pubblicitari relativi a prodotti o servizi commerciali, si è evoluto negli ultimi anni; alla pubblicità si sono così aggiunti altri messaggi potenzialmente pericolosi e ingannevoli, che possono causare malfunzionamenti della rete, nascondere frodi o veicolare la diffusione di virus e di altre forme di malware.

### **Un approccio coerente e coordinato allo spam**

Non esiste una soluzione semplice allo spam. La stessa ragione principale del successo di Internet, ovvero la sua natura aperta e decentralizzata, ha prodotto numerose vulnerabilità, che sono sfruttate in misura crescente dagli spammer e dai responsabili di altri illeciti *online*. La mancanza di un controllo centralizzato consente agli utenti di nascondere la propria identità. Inoltre, il basso costo dell'accesso a Internet e dei servizi di e-mail consente l'invio di milioni di messaggi al giorno con un costo marginale estremamente basso, in cui un tasso di risposta limitato consente di ottenere profitti elevati. Tuttavia si ritiene importante che la lotta allo spam e ad altre minacce *online* lasci inalterate le caratteristiche di apertura, flessibilità e innovazione alla base di Internet.

In questo contesto, all'inizio del suo mandato la Task Force ha dovuto prendere decisioni circa le azioni da promuovere e i ruoli dei diversi *stakeholder* nella lotta allo spam. Al riguardo, ha convenuto che il ruolo dei governi dovrebbe essere di formulare, di concerto con altre parti, chiare politiche nazionali antispam, collaborare con il settore privato e promuovere la cooperazione transfrontaliera. Si è inoltre

---

\*

convenuto sulla necessità, ai fini della lotta allo spam, di istituire gruppi di coordinamento nazionali e adeguati assetti regolamentari, sostenuti da obiettivi politici ben definiti e da efficaci meccanismi di controllo e sanzione. Si è riconosciuto che il settore privato ha un ruolo guida nello sviluppo di prassi operative e soluzioni tecniche innovative e può offrire un importante contributo all'educazione degli utenti. Il coordinamento e la cooperazione tra settore pubblico e operatori privati è di fondamentale importanza per sradicare il fenomeno dello spam.

In tale contesto, la Task Force contro lo spam ha sviluppato un kit di strumenti, con l'obiettivo di offrire ai paesi OCSE un orientamento di *policy* ampio e un quadro di riferimento coerente per la lotta allo spam, nella convinzione tuttavia che tale assetto possa essere applicabile e utile anche per i paesi non-OCSE. Il kit di strumenti è composto da 8 elementi collegati tra loro, che affrontano i seguenti aspetti:

**Approcci regolamentari:** lo sviluppo di una legislazione contro lo spam, che affronti il fenomeno e i problemi ad esso collegati, è di importanza fondamentale. Tale legislazione dovrebbe distinguere chiaramente ciò che è consentito da ciò che non lo è;

**Problemi di applicazione normativa:** oltre a una legislazione adeguata, la lotta allo spam si basa in misura fondamentale sulla disponibilità di adeguati strumenti per l'applicazione di tale legislazione. Un'azione efficace contro lo spam richiede tempestività e rapidità dell'azione di controllo e sanzione; per questo, nel mondo *online* molte procedure tradizionali hanno utilità ridotta, in quanto richiedono molte settimane o addirittura mesi. Un'attenzione particolare dovrebbe inoltre essere accordata al coordinamento nazionale, alle sanzioni, al conferimento di poteri adeguati alle autorità di controllo e alla cooperazione transfrontaliera;

**Iniziative settoriali:** per trattare in maniera adeguata il fenomeno dello spam, le normative nazionali antispam dovrebbero essere accompagnate da iniziative del settore privato;

**Soluzioni tecniche:** gli strumenti antispam operano a molti livelli – al punto di origine delle e-mail, a livello di dorsale e di gateway, e sul computer del destinatario – e possono essere usati da soli o in combinazione. Qualsiasi tentativo di combattere lo spam in modo efficace deve prevedere l'applicazione e la gestione ragionevole di diversi strumenti e metodi tecnologici. Nessun metodo può, da solo, garantire un'efficacia totale. L'uso congiunto ed efficace di diverse tecnologie antispam può ridurre drasticamente il livello di spam che colpisce un sistema;

**Educazione e consapevolezza:** una strategia antispam globale deve fare in modo che l'utente finale - ovvero il destinatario finale dello spam, la possibile vittima di virus e truffe, ma anche la persona in grado di controllare il proprio computer e i propri dati personali - sia sufficientemente consapevole del problema e informato su come affrontare lo spam e le altre minacce *online*. Ciò richiede attività di educazione e sensibilizzazione presso le grandi società, le piccole e medie imprese, gli utenti residenziali e le istituzioni scolastiche e formative. Tali attività dovranno essere finalizzate alla creazione di una cultura della sicurezza e incoraggiare un uso responsabile del ciber spazio;

**Partnership pubblico/privato contro lo spam:** gli enti pubblici e privati hanno un interesse comune ad assicurare la disponibilità e la sicurezza degli strumenti di comunicazione, al fine di promuovere lo sviluppo dell'economia digitale. La cooperazione tra settore pubblico e privato si svolge con una serie di modalità innovative. Esistono partnership strategiche, che operano di norma mediante attività di sensibilizzazione e condivisione delle informazioni. Partnership più operative contribuiscono all'educazione dell'utente, oltre che allo sviluppo (e all'applicazione) delle migliori prassi e allo scambio di informazioni e di dati nei casi di spam transfrontaliero. Inoltre, come testimoniato dalle attività a livello nazionale e internazionale, le partnership offrono uno strumento fondamentale per migliorare la

comunicazione e la comprensione reciproca di necessità, aspettative e problemi, promuovendo quindi la cooperazione e il reciproco coinvolgimento;

**Metriche:** la misurazione è essenziale per valutare l'evoluzione dello spam e l'efficacia delle soluzioni tecniche e degli sforzi formativi. Le metriche consentono di valutare le strategie nazionali e la loro attuazione, nonché di comprendere quali cambiamenti politici, regolamentari o tecnici sono necessari;

**Cooperazione globale:** come Internet, lo spam non conosce confini e si sposta senza ostacoli dalle economie sviluppate a quelle in via di sviluppo e viceversa. In tale contesto, la cooperazione globale è fondamentale per promuovere assetti di riferimento nazionali atti a neutralizzare lo spam in tutti i paesi e incoraggiare la cooperazione tra i governi, il settore privato, la società civile e le altre parti interessate. La cooperazione è necessaria per assicurare un'applicazione armonizzata e diffusa delle misure tecniche e un'efficace imposizione della normativa applicabile.

Per ognuno dei precedenti elementi, la Task Force raccomanda una serie di politiche e prassi:

### **Elemento I. Approcci regolamentari**

Lo sviluppo di una legislazione che affronti lo spam e i problemi ad esso connessi è di fondamentale importanza.

La normativa nazionale antispam dovrebbe mirare a:

1. **preservare i vantaggi della comunicazione elettronica**, promuovendo la fiducia degli utenti nei mezzi di messaggistica elettronica e in Internet, e migliorare l'offerta, l'affidabilità e l'efficienza dei servizi, nonché la prestazione delle reti di comunicazione globali;
2. **proibire e perseguire le attività di spamming, come definite dalla normativa nazionale.** L'esistenza di una normativa antispam potrà non essere di per sé sufficiente ad impedire ai potenziali spammer di avvalersi di tale tecnica di marketing. Nondimeno le leggi e le regole possono dare un contributo positivo prevedendo sanzioni per quelle persone, fisiche o giuridiche, che decidono di usare lo spam e di trarre benefici da esso. Il valore della legislazione dipenderà dalle sanzioni e, in particolare, dalla certezza della loro applicazione;
3. **ridurre il volume di spam.** Per impedire l'invio di spam, sarà necessario prevedere attività relative alle diverse fasi del processo di trasmissione, al fine di ridurre il volume di spam che attraversa le reti e il numero di messaggi indesiderati ricevuti dagli utenti finali.

Per il perseguimento di tali obiettivi, la legislazione dovrebbe conformarsi a quattro principi generali:

- **chiarezza di indirizzo:** la legislazione dovrebbe riflettere un chiaro indirizzo di *policy*. Le linee e gli obiettivi principali della politica antispam nazionale e internazionale dovranno essere delineati in una fase iniziale, e sottendere l'intera strategia di governo;
- **semplicità della regolamentazione:** la normativa dovrebbe essere breve e semplice;
- **efficacia del controllo:** l'applicazione della normativa è una questione di fondamentale importanza che, se non affrontata in modo adeguato, può rendere inutili anche le leggi migliori. Per questo, è importante creare un efficace sistema di sanzioni e criteri di prova adeguati. Le autorità preposte all'applicazione delle normative devono inoltre disporre di poteri e risorse adeguati;

- **collegamenti internazionali:** data la natura transfrontaliera dello spam, la legislazione dovrebbe prevedere dei collegamenti internazionali adeguati e consentire alle autorità nazionali di collaborare alle indagini e scambiare informazioni con le autorità estere (vedi sotto).

Nel valutare le migliori pratiche per la formulazione della normativa dovranno essere considerati, nella misura del possibile e tenendo conto dell'assetto istituzionale e giuridico del paese, i seguenti elementi:

	<b>Problema</b>	<b>Approccio</b>
<b>Ambito d'applicazione</b>	<b>Servizi</b>	<p>I formati tenderanno a convergere ed evolvere, ed è possibile che emergano tecnologie di messaggistica non prevedibili allo stato attuale</p> <p>Gli approcci normativi adottabili sono due:</p> <p>“approccio specifico” teso a disciplinare specifiche tecnologie di messaggistica, e più generalmente quelle che attualmente pongono problemi di spam;</p> <p>“approccio neutrale” teso a disciplinare le tecnologie di comunicazione in generale, in modo sufficientemente flessibile da accogliere evoluzioni tecnologiche future senza richiedere cambiamenti.</p> <p>I servizi voce in tempo reale dovrebbero essere disciplinati separatamente.</p>
	<b>Finalità</b>	<p>Valutare se la legislazione dovrà riguardare solo i messaggi commerciali o con finalità economica o se dovrà invece riguardare anche contenuti specifici non commerciali, quali i messaggi a contenuto politico o religioso.</p> <p>È possibile escludere espressamente categorie specifiche di messaggi dall'ambito di applicazione della normativa (per es. i messaggi di istituzioni accademiche ai propri studenti).</p>
<b>Consenso</b>	<b>Consenso</b>	<p>Il tipo di consenso o autorizzazione richiesto potrà variare a seconda dell'approccio regolamentare prescelto. Gli approcci al problema del consenso sono essenzialmente tre, spesso utilizzati insieme all'interno della legislazione:</p> <p>il consenso espresso, in cui un individuo o organizzazione ha attivamente autorizzato un'azione o attività particolare (<i>opt-in</i>);</p> <p>il consenso implicito, generalmente dedotto dalla condotta e/o da altre relazioni commerciali del destinatario;</p> <p>il consenso presunto; si presume il consenso fino a che questo non viene annullato dal destinatario, per esempio con l'opzione di “cancellazione” (<i>opt-out</i>).</p>
<b>Requisiti per la legittimità dei messaggi di marketing</b>	<b>Indirizzo di cancellazione</b> di	<p>I messaggi dovrebbero sempre comprendere una funzione di <i>opt-out</i>, che consente ai destinatari di annullare la propria sottoscrizione indicando il desiderio di non ricevere in futuro ulteriori comunicazioni dal mittente in questione.</p> <p>Ciò implica l'inclusione nell'e-mail di un indirizzo di risposta valido, in modo che il destinatario possa facilmente annullare la propria sottoscrizione. Possibile prevedere anche un indirizzo postale tradizionale.</p> <p>L'assenza di un'opzione di <i>opt-out</i>, di un indirizzo di risposta e di un indirizzo postale validi, nonché la mancata interruzione dell'invio di messaggi entro il periodo di tempo fissato dalla normativa dovrebbero essere oggetto di sanzione.</p>

	<b>Problema</b>	<b>Approccio</b>
	<b>Informazioni sull'origine del messaggio</b>	Una importante sfida in materia di disciplina e repressione dello spam proviene dall'abilità degli spammer di nascondere l'origine dei messaggi di spam inviati: <ul style="list-style-type: none"> <li>- la legislazione deve proibire l'invio di e-mail che falsificano l'origine o nascondono l'intestatario/l'identità del mittente;</li> <li>- la legislazione dovrebbe altresì richiedere una chiara identificazione dell'operatore di marketing collegato al mittente dell'e-mail.</li> </ul>
	<b>Non bulk</b>	La legislazione può prevedere che l'e-mail sia classificata come spam solo se è stato inviato un certo numero di messaggi in un determinato periodo di tempo (in genere più di 50-100 in 24 ore).  Questo elemento deve ovviamente tenere conto dell'esistenza di bulk e-mail (o e-mail di massa) legittime (per es. newsletter, ecc.).
	<b>Etichettatura</b>	La legislazione può imporre l'utilizzo di un'etichetta specifica per le e-mail contenenti materiale pubblicitario, pornografico ecc.
<b>Elementi ausiliari</b>	<b>Entità che autorizzano l'invio di spam o che aiutano/assistono lo spammer</b>	La normativa non dovrà sanzionare solo il mittente fisico, ma anche la persona che ha commissionato o autorizzato l'invio di messaggi o che ha tratto benefici finanziari dalle attività di spamming.  Questo approccio potrebbe facilitare l'applicazione della normativa, dal momento che, se è spesso difficile individuare il mittente dello spam, potrà invece essere più facile individuare chi beneficia dell'attività di spamming.
	<b>Tecniche di harvesting e liste di indirizzi raccolti in rete</b> <i>Dictionary attacks</i>	La legislazione potrà prevedere sanzioni aggiuntive qualora tali tecniche siano utilizzate per facilitare l'invio di spam in contrasto con la normativa in vigore; la vendita, l'acquisto o l'utilizzo di software di harvesting o di indirizzi raccolti in rete nonché la generazione automatica degli indirizzi dei destinatari potrà fare oggetto di sanzioni.
<b>Criminalità informatica e problemi di contenuto</b>	<b>Accesso illecito</b>	La legislazione dovrebbe impedire l'uso non autorizzato di risorse informatiche protette. La manipolazione di computer ai fini dell'invio di messaggi dovrebbe essere oggetto di sanzione.
	<b>Contenuti fuorvianti o fraudolenti</b>	Focus sui contenuti del messaggio, tralasciando i problemi sistemici dello spam.  Lo scam e il phishing possono configurarsi come reati informatici, ovvero reati ordinari ma perpetrati grazie a un sistema informatico. <ul style="list-style-type: none"> <li>- La legislazione antispam potrà integrare la normativa generale vietando l'uso di intestazioni fuorvianti o ingannevoli.</li> <li>- Potrà altresì disciplinare i contenuti, in particolare quando le normative antifrode, la legislazione sulla tutela dei consumatori ecc. non sono chiare al riguardo.</li> </ul>
	<b>Minacce alla sicurezza</b>	Gli aspetti di <i>malware</i> dello spam sono spesso sanzionati per via legislativa o possono essere sanzionati usando il quadro di riferimento della Convenzione del Consiglio d'Europa sulla criminalità informatica.

	<b>Problema</b>	<b>Approccio</b>
<b>Elemento internazionale</b>	<b>Giurisdizione transfrontaliera</b>	<p>La regolamentazione dovrebbe:</p> <ul style="list-style-type: none"> <li>• specificare la copertura di messaggi inviati a o dalla giurisdizione, nonché dei messaggi commissionati dall'interno della giurisdizione e dei benefici finanziari collegati allo spam;</li> <li>• assicurare che gli spammer siano sanzionati dalla normativa nazionale, anche se producono spam destinato ad altri paesi;</li> <li>• riconoscere alle autorità nazionali antispam il potere di cooperare a livello internazionale. Anche gli accordi sull'applicazione normativa transfrontaliera sono importanti.</li> </ul>

Anche il ruolo dei provider di servizi Internet e di e-mail è importante e potrà essere coperto dalla normativa. In particolare, i governi e le autorità di controllo dovranno favorire lo sviluppo di codici di migliori pratiche per gli ISP, che integrino la normativa e siano coerenti con essa. Dovranno altresì incoraggiare le associazioni di settore a sviluppare tali codici e ad adottare le migliori pratiche ove queste siano di interesse pubblico e non impongano indebiti oneri finanziari e amministrativi ai partecipanti. Gli allegati II e III del Rapporto contengono un accordo sulle migliori pratiche elaborato dal Business and Industry Advisory Committee (BIAC) e dal Messaging Anti-Abuse Working Group (MAAWG) nel quadro dei lavori della Task Force contro lo spam.

Ove opportuno, tali codici potranno essere depositati presso l'autorità nazionale antispam, in linea con le prassi e norme nazionali. Ciò consentirà all'autorità di imporre il rispetto del codice agli operatori, nei casi in cui l'associazione di settore non riesca a farlo.

La legislazione potrebbe altresì offrire un quadro di riferimento ampio a sostegno delle iniziative degli ISP intese a bloccare o limitare la circolazione di messaggi spam. I provider dovranno poter adottare misure difensive adeguate ed equilibrate per proteggere le proprie reti, oltre alle azioni legali contro gli spammer. Risultati analoghi potranno essere conseguiti mediante adeguate disposizioni contrattuali tra i provider e gli utenti.

## **Elemento II. Applicazione della normativa**

La legislazione deve assicurare che le autorità preposte all'applicazione della normativa antispam dispongano dei poteri necessari a garantire la loro efficacia. Su proposta della Task Force è stata approvata una **Raccomandazione del Consiglio sulla cooperazione transfrontaliera in materia di applicazione delle normative contro lo spam** (vedi riquadro), in base alla quale i governi dovranno potenziare la propria normativa al fine di:

- a) creare un quadro di riferimento nazionale di strumenti normativi, autorità e prassi per l'applicazione delle normative collegate allo spam;
- b) migliorare la capacità delle autorità di cooperare con le loro omologhe estere, garantendo agli organi nazionali la possibilità di condividere le informazioni pertinenti e fornire assistenza investigativa;
- c) migliorare le procedure di cooperazione, definire il grado di priorità delle richieste di assistenza e utilizzare le risorse e le reti comuni<sup>1</sup>;

- d)* sviluppare nuovi modelli di cooperazione tra le autorità antispam e le organizzazioni private interessate.

**RACCOMANDAZIONE DEL CONSIGLIO SULLA COOPERAZIONE TRANSFRONTALIERA  
IN MATERIA DI APPLICAZIONE DELLE NORMATIVE CONTRO LO SPAM**

(adottata dal Consiglio nella sua 1133<sup>ma</sup> sessione, il 13 aprile 2006)

IL CONSIGLIO,

Vista la Convenzione sull'Organizzazione per la cooperazione e lo sviluppo economico del 14 dicembre 1960, in particolare l'articolo 5 b);

Riconoscendo che lo spam compromette la fiducia dei consumatori, che a sua volta rappresenta una condizione necessaria allo sviluppo della società dell'informazione e del commercio elettronico;

Riconoscendo che lo spam può facilitare la diffusione di virus e veicolare frodi e truffe tradizionali, oltre che frodi informatiche come il phishing, e che i suoi effetti possono influire negativamente sulla crescita dell'economia digitale, imponendo dunque considerevoli costi economici e sociali ai paesi membri e alle economie dei paesi non membri;

Riconoscendo che lo spam pone delle sfide uniche in materia di controllo giacché il mittente di messaggi spam può facilmente nascondere la propria identità, falsificare il percorso elettronico di tali messaggi e inviarli da ovunque a chiunque nel mondo, rendendo lo spam un problema intrinsecamente internazionale, che può essere affrontato in modo efficace solo attraverso la cooperazione internazionale;

Riconoscendo la necessità di superare diverse sfide alla raccolta e condivisione delle informazioni tramite la cooperazione globale, identificando le priorità e sviluppando assetti internazionali efficaci per il controllo del fenomeno;

Riconoscendo che le misure esistenti, fra cui i numerosi strumenti di cooperazione bilaterale e multilaterale in materia penale, offrono già un quadro di riferimento per la cooperazione nella repressione di condotte criminose associate allo spam, fra cui il malware e il phishing;

Vista la Raccomandazione del Consiglio concernente le Linee guida sulla tutela dei consumatori contro le pratiche commerciali transfrontaliere fraudolente e ingannevoli ("*Cross border Fraud Guidelines*"), in cui vengono delineati i principi per la cooperazione tra le autorità nazionali preposte alla tutela dei consumatori contro le pratiche fraudolente e ingannevoli [C(2003)116];

Vista la Raccomandazione del Consiglio concernente le Linee guida che disciplinano la tutela della privacy e i flussi transfrontalieri di dati personali [C(80)58] ("*Privacy Guidelines*"), e la Dichiarazione ministeriale sulla tutela della privacy sulle reti globali (*Ministerial Declaration on the Protection of Privacy on Global Networks*) [C(98)177];

Riconoscendo che, in taluni casi, le suddette Linee guida possono essere applicate direttamente alla cooperazione transfrontaliera in materia e che, ove ciò non fosse possibile, molti principi ivi espressi possono essere adattati in modo utile al fine di sviluppare quadri nazionali adeguati e facilitare la cooperazione internazionale per l'applicazione della normativa contro lo spam;

Rammentando che, anche se la cooperazione internazionale è un elemento importante per affrontare il problema dello spam, è necessario che a livello nazionale vengano adottati approcci di ampio respiro che affrontino le problematiche regolamentari e di *policy*, agevolino lo sviluppo di soluzioni tecniche adeguate, promuovano l'educazione e la consapevolezza di tutte le parti in causa e incoraggino le iniziative di settore;

In base alla proposta congiunta del Comitato per la politica dell'informazione, dell'informatica e delle comunicazioni (ICCP) e del Comitato per la politica dei consumatori:

**CONVIENE che:**

Ai fini della presente raccomandazione e fatti salvi gli altri strumenti di cooperazione esistenti, per "Autorità competenti per l'applicazione delle normative contro lo spam" si intende qualsiasi organo pubblico nazionale, come stabilito da ogni paese membro, preposto all'applicazione delle normative collegate allo spam e che disponga di poteri per (a) coordinare o condurre indagini o (b) applicare sanzioni o (c) entrambi.

Ai fini della presente raccomandazione, per "Normative collegate allo spam" si intende (a) normative che riguardano in modo specifico le comunicazioni elettroniche; o (b) normative generali, quali la normativa sulla privacy, sulla tutela dei consumatori o sulle telecomunicazioni, che possono applicarsi alle comunicazioni elettroniche.

La presente raccomandazione è destinata principalmente agli organi nazionali pubblici, preposti all'applicazione delle normative collegate allo spam. Si riconosce che in alcuni paesi membri, diversi organi competenti, alcuni dei quali a livello regionale o locale, condividono il potere di intentare o promuovere azioni legali contro lo spam. Si riconosce altresì che, in taluni paesi membri, esistono organismi privati che contribuiscono in modo sostanziale ad assicurare l'applicazione delle normative collegate allo spam, anche in situazioni transfrontaliere.

La presente raccomandazione si applica alla cooperazione transfrontaliera per l'applicazione della normativa contro lo spam solo nei settori in cui la condotta proibita dalla normativa del paese membro che riceve una richiesta di assistenza è sostanzialmente simile alla condotta proibita dalle corrispondenti normative nel paese membro richiedente. La cooperazione ai sensi della presente raccomandazione non limita la libertà di espressione, come tutelata dalle leggi dei paesi membri.

La cooperazione ai sensi della presente raccomandazione si concentra sulle violazioni più gravi delle normative collegate allo spam, fra cui le violazioni che (a) causano o potrebbero causare danni (finanziari o di altro tipo) a un numero significativo di destinatari, (b) interessano un numero particolarmente elevato di destinatari, (c) causano danni sostanziali ai destinatari.

In tutti i casi, la decisione se fornire assistenza ai sensi della presente raccomandazione rimane di competenza dell'autorità antispam che riceve la richiesta.

I paesi membri sono esortati a collaborare in questo ambito anche sulla base di eventuali altri strumenti, accordi o disposizioni.

**RACCOMANDA che:**

I paesi membri si adoperino per promuovere una cooperazione più intensa, rapida ed efficiente tra le proprie autorità competenti per l'applicazione delle normative contro lo spam, prevedendo, ove

adeguato:

#### **a) la creazione di un quadro nazionale**

Al riguardo gli Stati membri dovrebbero:

(i) introdurre e mantenere un sistema efficace di strumenti normativi, autorità e prassi, per l'applicazione delle normative collegate allo spam;

(ii) adottare misure affinché le autorità antispam dispongano dei poteri necessari a svolgere attività di istruzione e accertamento nonché sanzionare in modo tempestivo le violazioni delle normative collegate allo spam che siano commesse o abbiano effetti sul proprio territorio. Tali poteri dovranno includere la capacità di ottenere le informazioni necessarie e la documentazione collegata;

(iii) migliorare la capacità delle autorità antispam di adottare provvedimenti opportuni contro (a) i mittenti di comunicazioni elettroniche che violano le normative collegate allo spam e (b) le persone, fisiche o giuridiche, che traggono profitti dall'invio di tali comunicazioni;

(iv) riesaminare periodicamente i propri assetti nazionali e adottare misure al fine di assicurare la loro efficacia ai fini della cooperazione transfrontaliera in materia di applicazione delle normative collegate allo spam;

(v) esaminare le modalità per migliorare gli strumenti per rimediare ai danni finanziari causati dallo spam.

#### **b) il potenziamento delle capacità di cooperazione**

I paesi membri dovrebbero potenziare l'abilità delle proprie autorità antispam di cooperare con le corrispondenti autorità estere.

Al riguardo i paesi membri dovrebbero:

(i) creare meccanismi che consentano alle proprie autorità antispam di condividere con le autorità estere, su loro richiesta, informazioni su violazioni delle loro normative antispam, ove opportuno e con le misure di sicurezza adeguate;

(ii) permettere alle proprie autorità antispam di fornire alle autorità estere, su loro richiesta, assistenza investigativa relativamente a violazioni delle loro normative antispam, ove opportuno e con le misure di sicurezza adeguate, in particolare riguardo all'ottenimento di informazioni da persone; l'ottenimento di documenti o registrazioni; il reperimento e identificazione di persone o cose;

(iii) nominare un punto di contatto per la cooperazione ai sensi della presente raccomandazione e fornire al Segretariato dell'OCSE informazioni aggiornate circa le proprie normative collegate allo spam e sull'autorità antispam nominata come punto di contatto. Il Segretariato dell'OCSE avrà cura di conservare tali informazioni, mettendole a disposizione delle parti interessate.

#### **c) il miglioramento delle procedure di cooperazione**

Prima di presentare richieste di assistenza come previsto nei precedenti paragrafi, le autorità antispam dovrebbero:

(i) avviare indagini preliminari per determinare se la richiesta di assistenza sia giustificata e coerente con l'ambito di applicazione e le priorità esposte nella presente raccomandazione;

(ii) definire il grado di priorità delle richieste di assistenza e, nei limiti del possibile, utilizzare risorse comuni quali il sito Internet dell'OCSE sullo spam, canali informali, reti internazionali esistenti e gli esistenti strumenti di cooperazione in materia di applicazione delle normative al fine di attuare la presente raccomandazione.

#### **d) la cooperazione con il settore privato**

Le autorità antispam, le imprese, le organizzazioni di settore e le associazioni dei consumatori sono esortate a cooperare per contrastare le violazioni della normativa antispam. In particolare, le autorità dovrebbero collaborare con tali gruppi perché questi partecipino ad iniziative per l'educazione degli utenti, favoriscano la segnalazione all'autorità di eventuali abusi e condividano con le autorità strumenti e tecniche investigative, analisi, dati e informazioni di lungo periodo sul fenomeno.

I paesi membri dovrebbero incoraggiare la cooperazione tra le autorità antispam e il settore privato al fine di facilitare l'individuazione e l'identificazione degli spammer.

I paesi membri dovrebbero altresì incoraggiare la partecipazione da parte del settore privato e delle economie di paesi non membri agli sforzi internazionali di cooperazione nell'applicazione delle normative, agli sforzi per ridurre la frequenza di imprecisioni nei dati sui proprietari di nomi di dominio e agli sforzi per aumentare la sicurezza di Internet.

Ove opportuno, le autorità antispam e il settore privato dovrebbero continuare a esplorare nuovi modi per contenere il fenomeno.

**INVITA** le economie dei paesi non membri a prendere in debita considerazione la presente raccomandazione e a collaborare con i paesi membri alla sua attuazione.

**INCARICA** il Comitato per la politica dell'informazione, dell'informatica e delle comunicazioni e il Comitato per la politica dei consumatori di monitorare i progressi nella cooperazione transfrontaliera in materia di applicazione delle normative ai sensi della presente raccomandazione entro tre anni dalla sua adozione e successivamente, come opportuno.

### **Elemento III. Iniziative di settore**

Per affrontare in modo adeguato il fenomeno dello spam, la normativa dovrà essere accompagnata da iniziative di autoregolamentazione degli operatori del settore privato, fra cui i provider di servizi Internet e di posta elettronica, gli operatori nel settore delle telecomunicazioni, gli operatori di marketing diretto, gli operatori *online*, le società di software e le loro associazioni.

Le iniziative del settore privato costituiscono una parte importante del quadro di riferimento per le politiche contro lo spam. La Task Force:

- accoglie con favore gli sforzi profusi da BIAC e MAAWG nel redigere le migliori pratiche e prende nota dei risultati raggiunti finora,
- incoraggia il loro continuo miglioramento, anche attraverso il dialogo con gli organismi preposti alle politiche antispam e alla regolamentazione,
- nota che le migliori pratiche evolveranno alla luce degli sviluppi regolamentari, tecnici e commerciali,
- nota che in talune giurisdizioni c'è la possibilità che dette migliori pratiche ricevano un riconoscimento formale.

Nello svolgimento delle loro attività **i fornitori di servizi e di beni *online*** dovrebbero promuovere iniziative per:

- sviluppare metodi e standard di comunicazione aziendale che rispettano la *privacy* dei clienti, gestendo con cura le informazioni personali e gli indirizzi di posta elettronica. L'adozione di standard aziendali relativi ai siti web, all'utilizzo di domini e alla messaggistica elettronica contribuisce a proteggere gli utenti. È necessario formulare e applicare con coerenza politiche aziendali chiare sulla posta elettronica – che prevedano per esempio di astenersi dal chiedere informazioni personali o, possibilmente, dall'inviare collegamenti cliccabili nel corpo dei messaggi elettronici. Una società che invia messaggi e-mail ai suoi clienti potrà valutare la possibilità di autenticarli o di utilizzare firme digitali;
- valutare iniziative preventive per ostacolare condotte criminose quali il phishing. Tali iniziative comprendono misure per ridurre la vulnerabilità del sito Internet aziendale, usando un nome di dominio chiaro e una politica di registrazione difensiva (per es. registrando nomi di dominio che, in quanto simili al proprio dominio aziendale, potrebbero creare confusione), il monitoraggio dell'uso del sito, il controllo dei messaggi rinviati al mittente, il monitoraggio di siti che imitano il proprio ecc.;
- educare e sensibilizzare i consumatori, offrire supporto ai clienti. Le società che operano *online* dovrebbero comunicare in modo efficace con i propri clienti, chiarendo le tipologie di comunicazioni che possono o saranno inviate via e-mail e le modalità con cui l'utente può accedere agli indirizzi e-mail e ad altri dati o modificarli, specificando che all'utente non verrà mai chiesto di fornire per e-mail i propri dati personali ed elencando le caratteristiche del messaggio che consentono di verificarne l'effettiva provenienza.

#### **Gli operatori di marketing diretto dovrebbero:**

- adottare e applicare un codice di condotta basato sulle migliori pratiche per il marketing elettronico, che riguardi anche l'invio di messaggi commerciali tramite posta elettronica, strumenti di messaggistica istantanea o cellulari. Tali associazioni, così come quelle che riuniscono gli operatori *online*, potranno stringere relazioni più strette con i provider di servizi Internet e con gli altri operatori di rete, al fine di ridurre il numero di falsi positivi, garantendo nel contempo la legittimità e correttezza delle proprie attività;
- adottare migliori pratiche o codici di condotta finalizzati ad agevolare e coadiuvare l'applicazione della legislazione antispam a livello nazionale e internazionale. A tal fine, i governi e le associazioni dovrebbero provvedere a diffondere i dati relativi ai diversi approcci legislativi.

La Task Force dell'OCSE nota che il BIAC ha sviluppato una serie di migliori pratiche e raccomandazioni sul marketing elettronico, allegate al Rapporto.

#### **I provider di servizi Internet e gli altri operatori di rete dovrebbero:**

- adottare e applicare degli strumenti di autoregolamentazione nella forma di migliori pratiche e codici di condotta;
- adottare e imporre una politica d'uso accettabile (PUA) che proibisca lo spamming e le attività ad esso collegate sulle proprie reti. Tali politiche potranno far parte degli accordi contrattuali tra il provider e l'utente, in modo che la loro violazione comporti una violazione degli obblighi contrattuali e consenta la sospensione del servizio e l'estinzione del contratto stesso;
- fornire agli abbonati informazioni sulla disponibilità, l'utilizzo e la corretta applicazione di software per filtrare spam e virus. Gli ISP sono esortati a fornire filtri e aggiornamenti a un prezzo ragionevole e a indicare agli utenti come procurarsi soluzioni *open source* antispam e antivirus.

I governi sono esortati ad incoraggiare i provider nazionali e gli altri operatori di rete ad adottare e attuare le migliori pratiche raccomandate. L'OCSE prende nota delle migliori pratiche per i provider dei servizi Internet e per gli altri operatori di rete sviluppate dal BIAC e MAAWG e disponibili nell'Allegato II del Rapporto.

**Gli operatori di telefonia mobile** dovrebbero adottare e applicare misure volte a ridurre la diffusione dello spam sulle proprie reti. La gamma di nuovi servizi offerti sui telefoni cellulari crea nuovi problemi simili allo spam per gli utenti di telefonia mobile. Fra le misure previste dagli dovrebbero figurare l'adozione di strumenti contrattuali, tecnici e informativi. La Task Force dell'OCSE prende nota delle migliori pratiche sviluppate dall'associazione GSM per gli operatori mobili (allegato IV al Rapporto).

#### **Elemento IV. Soluzioni tecniche**

I provider di servizi Internet e gli altri operatori di rete dovrebbero migliorare costantemente le proprie conoscenze e prassi operative e aggiornare le loro *best practices* tecniche, comprese quelle citate nell'elemento III, al fine di affrontare le nuove sfide poste dall'evoluzione tecnologica e promuovere l'attuazione e la condivisione di soluzioni tecniche tra provider. L'uso di diverse tecnologie antispam in collaborazione l'una con l'altra può ridurre drasticamente il livello di spam nel sistema. Anche se consentono di ridurre il quantitativo di spam nelle caselle di posta degli utenti, i filtri non sono di per sé sufficienti a ridurre il volume di spam che nasce da altre reti, rendendo necessaria l'adozione di un insieme di soluzioni tecniche.

#### **Elemento V. Iniziative di educazione e sensibilizzazione degli utenti**

##### ***Utenti residenziali:***

I governi dovrebbero:

- sviluppare campagne di informazione e di sensibilizzazione per educare gli utenti finali circa i prodotti e i servizi che utilizzano e i rischi associati, aiutandoli così a proteggersi dallo spam, dai virus e da altro malware. Queste informazioni dovrebbero essere anche disponibili sui portali dei provider;

- organizzare campagne di portata nazionale per attirare l'attenzione dei media e del grande pubblico;
- lavorare con il settore privato, la società civile e altre parti interessate a campagne di educazione degli utenti.

In virtù del loro rapporto diretto con gli utenti, i provider e gli altri operatori di rete, fra cui gli operatori di telefonia mobile, dovrebbero utilizzare i propri canali di comunicazione con i consumatori (siti web, portali, sms, newsletter) per offrire informazioni su:

- come evitare lo spam e i rischi associati a e-mail, SMS, MMS ecc.;
- filtri antispam e antivirus disponibili e soluzioni *open source*;
- come denunciare abusi ai provider o all'operatore, e alle autorità competenti;
- come contattare (via posta elettronica o telefono) dell'ufficio del provider cui segnalare abusi di servizio.

#### **Gruppi di utenti:**

- I corsi di computer per i **cittadini più anziani**, possibilmente finanziati dal governo o dagli enti locali, dovrebbero offrire informazioni sulla sicurezza informatica ed esempi pratici su come evitare lo spam, le frodi *online*, i virus e altro malware;
- I corsi di computer per **studenti e bambini** dovranno informare sulle minacce *online* e altre problematiche di sicurezza. La comunicazione con gli utenti più giovani potrà essere migliorata usando cartoni animati e fumetti.

#### **Grandi, piccole e medie imprese:**

- **Grandi imprese:** i dipartimenti di IT dovranno distribuire fra i nuovi assunti un documento che spiega la politica di sicurezza della società in materia di e-mail, i filtri esistenti e le migliori pratiche per affrontare il problema dello spam ed evitare di esserne vittima. Lo stesso tipo di informazioni dovrebbe essere disponibile sull'intranet; gli aggiornamenti andranno inviati periodicamente agli utenti;
- **PMI:** le associazioni di settore, i provider e le società che sviluppano software di sicurezza dovrebbero fornire alle PMI informazioni specifiche sulla disponibilità di pratiche semplificate per la gestione della sicurezza, di materiale di formazione, di software gratuito di tipo *open source*, ecc. Esempi e materiali sono disponibili sul sito Internet della Task Force dell'OCSE [www.oecd-antispam.org](http://www.oecd-antispam.org).

**L'educazione dei destinatari è importante quanto quella dei mittenti.** Le autorità di regolamentazione e le associazioni di categoria possono contribuire in modo considerevole alla formazione delle imprese, diffondendo informazioni su come comunicare con i clienti usando sistemi di messaggistica elettronica, quali l'e-mail, nel rispetto della normativa nazionale.

**Le associazioni di marketing diretto** dovrebbero informare i propri membri sulla legislazione antispam in vigore nel paese di origine e nel paese di destinazione del messaggio. Sarà inoltre utile coordinare a livello internazionale lo sviluppo di migliori pratiche e pagine web informative.

## **Elemento VI. Partnership pubblico/privato**

Qualsiasi strategia antispam dovrebbe essere sviluppata e attuata nel contesto di partnership fra pubblico e privato, con la partecipazione di rappresentanti di entrambi i settori. Perché le misure antispam siano efficaci è necessario che tutte le parti interessate siano coinvolte nella loro elaborazione, le accettino (con tutti i loro effetti secondari) e le considerino adeguate alle proprie necessità.

Le migliori pratiche, sviluppate dalle associazioni di settore con l'*input* delle autorità pubbliche, dovrebbero ricevere un'ampia applicazione. Tali migliori pratiche dovrebbero essere diffuse in modo capillare e attuate, oltre che aggiornate ove opportuno, per tenere conto dell'evoluzione del contesto tecnologico e dei servizi (vedi anche Elemento III).

L'industria e le autorità sono esortate a cooperare nell'attuazione della legislazione antispam. In particolare, i provider di servizi Internet e gli altri operatori di rete dovrebbero mantenere contatti con le autorità, per segnalare possibili casi di spam, e condividere con loro le informazioni sulle attività di spam nella loro rete.

## **Elemento VII. Metriche**

I governi e gli operatori del settore privato dovrebbero monitorare l'impatto delle misure antispam per valutarne l'efficacia. I provider, gli altri operatori di rete e le autorità nazionali antispam dovrebbero, nella misura possibile, condividere informazioni e dati sull'intensità e portata del fenomeno, nonché sulla sua evoluzione. I metodi di misurazione dovrebbero essere dettagliati e documentati, al fine di migliorare la leggibilità dei risultati ottenuti. In tale contesto il MAAWG ha sviluppato il suo sistema di metriche per le e-mail (E-mail Metrics Program). La Task Force accoglie con favore l'iniziativa e ne incoraggia il proseguimento e lo sviluppo.

## **Elemento VIII. Cooperazione globale**

La Task Force contro lo spam raccomanda che il presente kit di strumenti e le migliori pratiche indicate nel presente documento siano resi ampiamente disponibili anche nelle economie dei paesi non membri, oltre che all'interno dei paesi OCSE, e che tali risorse siano accessibili al massimo numero di persone possibile. In tale contesto, la Task Force ha sviluppato un sito Internet, consultabile all'indirizzo [www.oecd-antispam.org](http://www.oecd-antispam.org). Per assicurare che il sito Internet continui a costituire una risorsa utile e aggiornata, i paesi dovranno fornire regolarmente contributi, nonché nuovo materiale e notizie sulle proprie iniziative antispam a livello nazionale.

I paesi membri dell'OCSE sono esortati a promuovere ed agevolare le attività antispam in altri paesi attraverso partnership – accordi bilaterali o multilaterali, condivisione di informazioni, ecc. – al fine di contribuire allo sviluppo di un'adeguata legislazione antispam, promuovere l'applicazione di soluzioni tecniche e la diffusione di strumenti e risorse educative.

---

<sup>1</sup> Cfr. anche nell'Allegato V il LAP/EU CNSA Spam Complaint Referral (documento di lavoro) finalizzato a facilitare le richieste di assistenza e la segnalazione di indagini contro lo spam ad un'altra autorità partecipante.