COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 15.11.2006
COM(2006) 688 definitivo

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

Sulla lotta contro le comunicazioni commerciali indesiderate (*spam*), i programmi spia (*spyware*) e i software maligni

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

Sulla lotta contro le comunicazioni commerciali indesiderate (*spam*), i programmi spia (*spyware*) e i software maligni

(Testo rilevante ai fini del SEE)

1. SCOPO DELLA COMUNICAZIONE

La società civile constata ogni giorno di più l'importanza delle reti e dei servizi moderni di comunicazione elettronica per la vita quotidiana, sul lavoro o a casa. Per essere ampiamente adottati, tali servizi devono basarsi su tecnologie affidabili, sicure e degne di fiducia. La comunicazione della Commissione su una strategia per una società dell'informazione sicura[1] è finalizzata a migliorare la sicurezza delle reti e dell'informazione in generale e invita il settore privato a correggere le vulnerabilità presenti nelle reti e nei sistemi informatici che possono essere sfruttate per la diffusione di spam e di software maligni. La comunicazione della Commissione sul riesame del quadro normativo comunitario per le reti ed i servizi di comunicazione elettronica propone nuove regole per rafforzare la sicurezza e la riservatezza nel settore delle comunicazioni elettroniche[2].

La presente comunicazione affronta l'evoluzione dello spam[3] e le minacce rappresentate dai programmi spia e dai software maligni. Oltre a fare il punto delle azioni intraprese fino ad ora per combattere queste minacce la comunicazione individua ulteriori provvedimenti possibili, quali:

- il rafforzamento della legislazione comunitaria,

- l'attività diretta a far osservare la legge

- la cooperazione all'interno degli Stati membri e tra Stati membri,

- il dialogo politico ed economico con i paesi terzi,

- le iniziative delle imprese del settore,

- le attività di R&S.

---

1 COM(2006) 251.definitivo
2 COM(2006) 334 definitivo
3 COM(2004) 28.definitivo

2. IL PROBLEMA – MUTEVOLEZZA DELLE MINACCE

Lo spam[4] è aumentato considerevolmente negli ultimi cinque anni[5]. Fonti del settore riferiscono che lo spam rappresenta ormai tra il 50 e l'80% dei messaggi indirizzati agli utilizzatori finali[6]. Sebbene la maggior parte dello spam provenga dal di fuori dell'UE, i paesi europei trasmettono oggi il 25% dei messaggi indesiderati[7]. A livello mondiale il costo dello spam è stato stimato a 39 miliardi di euro nel 2005, mentre in Europa, il suo costo per le principali economie è stimato a circa 3,5 miliardi di euro in Germania, 1,9 miliardi di euro nel Regno Unito e 1,4 miliardi di euro in Francia[8]. L'invio di spam è considerato una vera e propria attività commerciale. I professionisti dello spam (*spammer*) noleggiano o vendono alle società di marketing gli elenchi di indirizzi elettronici che hanno raccolto. Lo spam in internet è particolarmente redditizio, grazie alla portata di questo mezzo di comunicazione e al costo limitato che comporta l'invio massiccio di messaggi. Contemporaneamente, con investimenti anche moderati nella lotta contro lo spam si possono ottenere risultati significativi. Nei Paesi Bassi, ad esempio, è stato possibile ridurre dell'85% lo spam in neerlandese investendo **570 000 euro** in apparecchiature per la lotta antispam.

Da semplice fastidio, i messaggi di posta elettronica indesiderati sono divenuti poco a poco un atto di natura fraudolenta e delittuosa. Un esempio lampante è costituito dalla pratica del *phishing*, vale a dire l'invio di messaggi di posta elettronica che inducono l'utilizzatore finale a visitare siti internet contraffatti che assomigliano ai siti di imprese reali e a rivelare presso tali siti dati riservati, con il grave pericolo di furti di identità e danni alla reputazione delle imprese legittime. Continua ad aumentare, inoltre, la diffusione, attraverso la posta elettronica o i programmi software, di programmi spia (*spyware*) che registrano e riferiscono il comportamento in linea degli utilizzatori. I programmi spia possono inoltre raccogliere informazioni personali quali password e numeri di carta di credito.

L'invio massiccio di messaggi di posta elettronica indesiderati è enormemente facilitato dalla diffusione di codici maligni quali worm e virus. Una volta installati, questi consentono a un aggressore di assumere il controllo di un sistema infetto e di trasformarlo in un "bot", parte di una rete "botnet"[9], in grado di nascondere l'identità del vero professionista dello spam. Le botnet sono noleggiate dai professionisti dello spam, del phishing e dai distributori di programmi spia per finalità fraudolente e delittuose. Gli esperti del settore stimano che le botnet trasmettano oltre il 50% dei messaggi di posta elettronica abusivi[10]. La diffusione dei programmi spia e di altri tipi di codici maligni di cui sono vittima i singoli cittadini e le

---

4 Per spam si intende l'invio di comunicazioni indesiderate - ad esempio, per posta elettronica - a fini commerciali. I messaggi di posta elettronica indesiderati, tuttavia, possono anche contenere software maligno e programmi spia.

5 Nel 2001 lo spam rappresentava il 7% del traffico di posta elettronica complessivo.

6 Symantec 54%; Messagelabs 68,6; MAAWG 80-85.

7 Primo trimestre 2006 (Sophos) Asia 42,8%, America settentrionale 25,6, Europa 25,0, America meridionale, 5,1, Australasia 0,8, Africa 0,6, Altri 0,1.

8 Ricerca Ferris, 2005.

9 Le "botnet" sono reti di computer, la cui sicurezza è stata compromessa, utilizzate dai professionisti dello spam per inviare massicci quantitativi di posta elettronica attraverso l'installazione di software nascosto che trasforma tali computer in server di posta ad insaputa dell'utilizzatore.

10 Classifica dei paesi con il maggior numero di botnet secondo Symantec (3° e 4° trimestre 2005): Stati Uniti 26%, Regno Unito 22%, Cina 9%, Francia, Corea del Sud e Canada 4%, Taiwan, Spagna e Germania 3%, Giappone 2%.

imprese ha un impatto economico considerevole. L'impatto finanziario dei software maligni a livello mondiale è stato stimato attorno agli 11 miliardi di euro nel 2005[11].

3. CIÒ CHE È STATO FATTO FINO AD ORA – AZIONI INTRAPRESE DAL 2004

Nel 2002 l'UE ha adottato una **direttiva relativa alla vita privata e alle comunicazioni elettroniche** che **vieta le comunicazioni indesiderate**[12] introducendo il principio del marketing basato sul consenso delle persone fisiche. Nel gennaio 2004 la Commissione ha presentato una comunicazione sullo spam che elencava le azioni destinate a integrare la direttiva[13]. Tale comunicazione sottolineava la necessità di varare azioni a vari livelli in materia di sensibilizzazione, di autoregolamentazione, di soluzioni tecniche, di cooperazione e di applicazione della legislazione. La Commissione ha cominciato ad affrontare la questione della lotta contro lo spam, i programmi spia e i software maligni nell'ambito delle discussioni con i paesi terzi. Inoltre, la direttiva sulle pratiche commerciali sleali[14] protegge i consumatori dalle pratiche commerciali aggressive; la cooperazione transfrontaliera per la lotta contro tali pratiche è contemplata dal regolamento sulla cooperazione per la tutela dei consumatori[15].

3.1. Azioni di sensibilizzazione

La comunicazione della Commissione ha contribuito a sensibilizzare gli utilizzatori al problema dello spam a livello nazionale e internazionale. A livello dell'UE, il **programma Safer Internet *plus*** promuove un utilizzo più sicuro di internet e delle nuove tecnologie on-line, in particolare da parte dei bambini, nell'ambito di una strategia coerente dell'Unione europea.

Gli Stati membri hanno avviato o sostenuto **campagne** di sensibilizzazione degli utilizzatori ai problemi dello spam e ai mezzi per porvi rimedio. In generale i fornitori del servizio internet (ISP) si sono incaricati di fornire ai loro clienti consigli e assistenza circa le modalità per proteggersi dai programmi spia e dai virus. Nel febbraio 2004 la Commissione ha ospitato un **seminario** dell'OCSE dedicato allo spam. La Commissione ha inoltre contribuito attivamente all'elaborazione del **Toolkit antispam** (Anti-Spam Toolkit) dell'OCSE, che costituisce un pacchetto completo di approcci normativi, soluzioni tecniche e iniziative del settore per la lotta contro lo spam.

Al vertice mondiale sulla società dell'informazione delle Nazioni Unite[16] è stato **riconosciuto** che lo spam deve essere affrontato ai livelli nazionale e internazionale appropriati. Nel 2004 e nel 2005 l'UIT (Unione internazionale delle telecomunicazioni) ha organizzato riunioni tematiche del WSIS. Da ultimo, l'agenda di Tunisi del WSIS, adottata nel novembre 2005, invita ad affrontare efficacemente il problema grave e sempre più preoccupante dello spam[17].

3.2. Cooperazione internazionale

Lo spam è un problema a valenza transnazionale e per questo sono state avviate numerose iniziative di cooperazione e sono stati istituiti svariati meccanismi di controllo

---

11 *Computer Economics: the 2005 Malware Report*.
12 Articolo 13 della direttiva 2002/58/CE.
13 *Supra* 3.
14 Allegato 1, punto 26 della direttiva 2005/29/CE.
15 Regolamento (CE) 2006/2004.
16 WSIS, Ginevra, dicembre 2003.
17 Agenda di Tunisi, paragrafo 41.

dell'applicazione della legge a livello transfrontaliero. La Commissione ha creato una **rete di contatto delle autorità antispam** (CNSA, Contact Network of Spam Authorities) che si riunisce regolarmente, scambia le buone pratiche e coopera sull'applicazione transfrontaliera della legge. Il CNSA ha redatto una procedura di cooperazione[18] per agevolare il trattamento transfrontaliero delle denunce relative allo spam. I servizi della Commissione sostengono e partecipano in qualità di osservatori al **piano d'azione di Londra** (LAP, London Action Plan) che raggruppa le autorità incaricate di fare applicare la legge di venti paesi e ha inoltre adottato una procedura di cooperazione transfrontaliera. Un seminario congiunto CNSA UE – LAP si è tenuto nel novembre 2005. Nell'aprile 2006 l'**OCSE** ha adottato una raccomandazione relativa alla cooperazione transfrontaliera nell'applicazione delle leggi antispam che incoraggia le autorità competenti a scambiarsi informazioni e a collaborare[19].

La Commissione incoraggia inoltre le **iniziative di cooperazione internazionale**. Gli Stati Uniti e l'Unione europea hanno convenuto di cooperare per affrontare il problema dello spam attraverso iniziative congiunte di applicazione della legge e per studiare i mezzi di lotta contro i programmi spia e i software maligni illeciti. La Commissione partecipa inoltre al gruppo di lavoro sullo spam nell'ambito della collaborazione internazionale del Canada (Canadian International Collaboration). Sono in corso colloqui con i principali partner internazionali quali la Cina e il Giappone. Per quanto riguarda l'Asia, la Commissione ha preso l'iniziativa di una dichiarazione congiunta sulla cooperazione internazionale antispam che è stata adottata alla conferenza dell'ASEM sul commercio elettronico nel febbraio 2005[20].

L'agenda di Tunisi, adottata nel novembre 2005 dal vertice mondiale sulla società dell'informazione (WSIS), sottolinea che la sicurezza di internet è un settore che esige una migliore collaborazione internazionale e che la questione dovrà essere affrontata nell'ambito del modello di cooperazione rafforzata per la governance di internet che sarà attuato come seguito al vertice[21].

3.3. Ricerca e sviluppo tecnologico

Nell'ambito del Sesto programma quadro RST, la Commissione ha avviato progetti per aiutare i soggetti interessati a combattere lo spam e altre forme di software maligni. Questi progetti[22] spaziano dal controllo generale delle reti e dalla rilevazione di attacchi all'elaborazione di tecnologie specifiche di filtraggio in grado di rilevare lo spam, le attività di phishing e i software maligni. Tra i risultati ottenuti si possono citare la creazione di una comunità di ricerca specializzata nel contenimento dei software maligni e lo sviluppo di un'infrastruttura europea per il monitoraggio del traffico in internet. Le attività intraprese di recente riguardano filtri adattativi in grado di rilevare le minacce sconosciute e i cyberattacchi. Lo sforzo finanziario consacrato a tali attività ammonta a 13,5 milioni di euro.

---

18 http://europa.eu.int/information_society/policy/ecomm/doc/todays_framework/privacy_protection/spam/cooperation_procedure_cnsa_final_version_20041201.pdf

19 http://www.oecd-antispam.org/

20 http://www.asemec-london.org/

21 Agenda di Tunisi, paragrafi da 39 a 47. http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc

22 www.diademhttp://cordis.europa.eu/fp6/projects.htm#search

3.4. Attività delle imprese

La Commissione si compiace del ruolo proattivo svolto dalle imprese in materia di spam. I fornitori di servizi hanno, in generale, adottato **misure tecniche** per affrontare lo spam, in particolare filtri antispam più avanzati. Gli ISP hanno istituito un **supporto tecnico** che fornisce agli utilizzatori software contro lo spam, i programmi spia e i software maligni. Numerosi ISP prevedono **clausole contrattuali** che vietano i comportamenti illeciti on-line. Recentemente, un tribunale britannico ha inflitto un'ammenda di 68 800 euro a un professionista dello spam per inadempienza contrattuale. Le associazioni del settore hanno adottato una serie di buone pratiche per prevenire il phishing on-line e migliorare i metodi di filtraggio[23].

Anche gli operatori della telefonia mobile si sono impegnati in tal senso e i codici di condotta professionale prevedono la possibilità di adottare provvedimenti contro i messaggi indesiderati. L'associazione GSM ha pubblicato, nel 2006, un codice di buone pratiche contro lo spam nelle comunicazioni mobili. Attualmente la Commissione cofinanzia l'iniziativa Spotspam – un partenariato tra enti pubblici e privati finalizzato alla creazione di una base dati che agevoli le indagini transfrontaliere e l'applicazione della legge nei casi di spam[24].

3.5. Misure per l'applicazione della legge

È evidente che l'impegno nella lotta contro lo spam dà risultati. Le misure di filtraggio imposte in Finlandia hanno permesso di far scendere la percentuale di spam nei messaggi elettronici dall'80% al 30%. Numerose autorità competenti hanno intrapreso iniziative per fermare i professionisti dello spam[25].

Esistono, tuttavia, differenze significative tra gli Stati membri quanto al numero reale di casi perseguiti. In alcuni paesi le autorità hanno aperto almeno un centinaio di indagini che sono state condotte a buon fine e hanno permesso di sanzionare le attività di invio di spam. In altri Stati membri, le indagini hanno riguardato al massimo cinque casi e talvolta nessuno.

La maggior parte delle azioni ha riguardato le **forme "tradizionali"** di spam. **Le altre minacce segnalate hanno raramente dato luogo ad azioni penali**, pur avendo provocato grandi rischi.

4. IL LAVORO CHE RESTA DA FARE IN FUTURO

4.1. Azione a livello degli Stati membri

Questa sezione riguarda le azioni che spettano ai poteri pubblici e alle autorità nazionali, in particolare per quanto riguarda l'applicazione della legge e la cooperazione.

---

23 http://www.maawg.org/home/

24 http://www.spotspam.net

25 Un sondaggio della CNSA mostra che quindici dei diciotto membri che hanno partecipato al sondaggio hanno perseguito casi nel periodo 2003-2006.

4.1.1. Fattori chiave del successo

La persistenza e la mutevolezza del problema esigono un maggior coinvolgimento da parte degli Stati membri, che devono fissare una scala di priorità. In particolare, le azioni devono concentrarsi, da un lato, sui professionisti dello spam e del phishing e, dall'altro, sulla diffusione di programmi spia e software maligni. Gli strumenti decisivi per il successo sono:

– un forte impegno da parte del governo centrale nella lotta contro le pratiche illecite on-line;

– una chiara attribuzione delle responsabilità organizzative delle attività di controllo dell'applicazione della legge;

– la stanziamento di risorse adeguate per le attività di tali autorità.

Al momento questi fattori non sono presenti in tutti gli Stati membri.

4.1.2. Coordinamento e integrazione a livello nazionale

In base alla direttiva relativa alla vita privata e alle comunicazioni elettroniche e alla direttiva relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali[26], le autorità nazionali sono competenti a perseguire le pratiche illecite consistenti:

- nell'inviare comunicazioni indesiderate (**spam**)[27];

- nell'accedere illegalmente alle apparecchiature terminali per memorizzarvi informazioni, quali **software pubblicitari o programmi spia**, oppure per accedere alle informazioni memorizzate su tali apparecchiature[28];

- nell'infettare apparecchiature terminali inserendo **software maligni** quali worm e virus e trasformare i computer in **bot** o utilizzarli per altri fini[29];

- nell'indurre con l'inganno gli utilizzatori a rivelare informazioni riservate[30], quali password e numeri di carte di credito, attraverso messaggi cosiddetti di **phishing**.

Alcune di queste pratiche sono penalmente perseguibili, come dispone la *decisione quadro relativa agli attacchi diretti contro i sistemi di informazione*[31]. Secondo tale decisione, gli Stati membri devono prevedere una pena carceraria di almeno tre anni, o di cinque anni se il reato è commesso nell'ambito della criminalità organizzata.

A livello nazionale l'osservanza di tali disposizioni può essere assicurata da autorità amministrative o dalle autorità giudiziarie in sede penale. In tal caso, devono essere chiaramente definite le **responsabilità** delle singole autorità e le procedure di cooperazione. Per far questo possono essere necessarie decisioni assunte dai governi ai massimi livelli.

---

26 Direttiva 95/46/CE.

27 Articolo 13 della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

28 Articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

29 *Supra* 28.

30 Articolo 6, lettera a), della direttiva relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali.

31 Decisione quadro 2005/222/JHA del Consiglio.

Fino ad oggi, alla crescente commistione tra gli aspetti penali e amministrativi dello spam e delle altre minacce in linea non hanno fatto riscontro progressi nelle procedure di cooperazione tra gli Stati membri, tali da unire le competenze tecniche e investigative delle varie agenzie. È necessario istituire protocolli di cooperazione in settori come lo scambio di informazioni e di intelligence, i punti di contatto, l'assistenza e l'attribuzione di casi.

La stretta cooperazione tra le autorità incaricate di fare applicare la legge, gli operatori di rete e gli ISP a livello nazionale risulta vantaggiosa anche per lo scambio di informazioni e competenze tecniche e per perseguire le pratiche illecite in linea. Le autorità della Norvegia e dei Paesi Bassi hanno confermato l'utilità di questo partenariato pubblico-privato.

4.1.3. Risorse

Sono necessarie risorse per raccogliere prove, condurre indagini e perseguire i reati. Le autorità necessitano di risorse tecniche e giuridiche e devono familiarizzarsi con il *modus operandi* dei criminali per riuscire a far cessare le loro pratiche.

I meccanismi di denuncia on-line, con i relativi sistemi per la registrazione e l'analisi delle pratiche illecite comunicate, possono rivelarsi uno strumento importante. L'esperienza ha mostrato che **investimenti anche modesti** possono produrre **risultati significativi**. Lo spam in neerlandese è stato ridotto creando un gruppo di cinque dipendenti dell'OPTA, l'autorità olandese competente, impegnati a tempo pieno e dotati di apparecchiature del valore di **570 000 euro** per la lotta antispam. A partire da questo investimento, l'esperienza acquisita nella lotta antispam è ora utilizzata in altri settori problematici.

4.1.4. Cooperazione transfrontaliera

Lo spam è un problema globale. Le autorità nazionali dovranno spesso affidarsi alla collaborazione delle autorità di altri paesi per perseguire i professionisti dello spam o, viceversa, potranno essere invitate a proseguire le indagini avviate in altri paesi.

Benché ci possa essere una certa riluttanza a impegnare le già scarse risorse nazionali per indagare su problemi di altri, è importante che gli Stati membri riconoscano che una cooperazione transfrontaliera efficace è fondamentale nella lotta contro lo spam. Di recente, le autorità australiane e olandesi competenti per la lotta contro lo spam hanno cooperato per smantellare un'importante centrale di spam.

Fino ad oggi sono 21 le autorità europee hanno approvato la procedura di cooperazione della CNSA[32] per la gestione transfrontaliera delle denunce; le restanti autorità sono invitate a fare altrettanto nei prossimi mesi. In particolare, gli Stati membri e le autorità competenti sono invitati a promuovere attivamente l'utilizzo:

- dei documenti pro forma comuni CNSA-LAP

- della raccomandazione e del toolkit dell'OCSE sull'applicazione della legge antispam.

4.1.5 Azioni proposte

---

32 *Supr*a 18.

Gli Stati membri e le autorità competenti sono invitati a:

- definire chiare linee di responsabilità per le agenzie nazionali impegnate nella lotta contro lo spam;

- garantire un coordinamento efficace tra le autorità competenti;

- coinvolgere i soggetti attivi sul mercato a livello nazionale, sfruttando le loro competenze e le informazioni disponibili;

- assicurare che siano stanziate risorse sufficienti per far rispettare la normativa;

- attenersi alle procedure di cooperazione internazionale e rispondere alle richieste di assistenza transfrontaliera.

4.2. Azione da parte del settore

In questa sezione sono illustrate le iniziative che il settore può avviare per rafforzare la fiducia dei consumatori e ridurre il fenomeno dell'invio di messaggi di posta elettronica illeciti

4.2.1. Trasmissione e installazione di software

I programmi spia costituiscono una grave minaccia per la vita privata degli utilizzatori. L'offerta di software in linea è divenuta un metodo molto comune per **trasmettere e installare programmi spia** sulle apparecchiature terminali degli utilizzatori. I programmi spia possono inoltre essere nascosti all'interno del software distribuito attraverso altri supporti, quali i CD-ROM utilizzati per l'installazione di programmi su un computer. I programmi spia indesiderati possono essere installati insieme ai programmi software acquistati dai consumatori.

Per impedire che i programmi spia raggiungano gli utilizzatori finali è necessario attuare le azioni specifiche illustrate di seguito.

4.2.2. Informare il consumatore

I programmi software che si acquistano possono comprendere l'installazione di programmi aggiuntivi. Se il software agisce come spyware tenendo traccia del comportamento degli utilizzatori finali (ad esempio per finalità di marketing), presuppone l'elaborazione di dati personali ed è pertanto illegale in assenza del consenso informato da parte dell'utilizzatore. In moltissimi casi il consenso dell'utilizzatore all'installazione del software non viene richiesto oppure la richiesta è nascosta tra gli articoli di un lungo contratto di licenza per l'utilizzatore finale, scritto in caratteri minuscoli.

Le società che offrono prodotti software sono incoraggiate a descrivere in termini chiari e in caratteri ben leggibili tutti i termini e le condizioni dell'offerta, in particolare nel caso in cui siano inclusi nei pacchetti software dispositivi di monitoraggio che elaborano dati personali.

Per distinguere le imprese affidabili da quelle che non lo sono si potrebbe ricorrere all'autoregolamentazione e all'uso di un apposito "marchio di approvazione". I codici di condotta, finalizzati ad informare l'utilizzatore sulle condizioni che implica il trattamento dei dati personali, possono essere presentati per approvazione al Gruppo per la tutela dei dati

personali con riguardo al trattamento dei dati personali, istituito a norma dell'articolo 29 (della direttiva 95/46/CE).

4.2.3 Clausole contrattuali nella filiera della distribuzione

Spesso le imprese **non sono a conoscenza** delle modalità tecniche con cui i loro prodotti e i loro servizi sono pubblicizzati presso il pubblico. All'interno di programmi software legittimi possono essere inseriti programmi spia utilizzati per accedere a dati riservati, quali numeri di carte di credito, documenti riservati ecc.

Le imprese che pubblicizzano o vendono prodotti devono accertarsi che le attività delle controparti contrattuali siano legittime. Un'impresa deve avere una visione chiara delle proprie relazioni contrattuali, accertarsi che la normativa sia rispettata e prevedere la risoluzione dei contratti per sanzionare pratiche scorrette, in modo da interrompere immediatamente ogni rapporto con le imprese che si sono rese colpevoli di scorrettezze.

4.2.4. Misure di sicurezza da parte dei fornitori di servizi

Un sondaggio dell'ENISA condotto nel 2006[33] conferma che, in generale, i fornitori di servizi hanno adottato provvedimenti antispam, ma osserva che potrebbero contribuire di più alla sicurezza complessiva della rete e raccomanda loro di prestare maggiore attenzione al filtraggio dei messaggi di posta elettronica che escono dalla loro rete (**filtraggio in uscita**, *egress filtering*). La Commissione incoraggia i fornitori di servizi ad attuare tale raccomandazione.

Gruppo per la tutela dei dati personali con riguardo al trattamento dei dati personali, istituito a norma dell'articolo 29 della direttiva citata ha adottato un parere sui problemi di riservatezza legati alla fornitura di servizi di cernita della posta elettronica[34] che fornisce indicazioni sulla questione della riservatezza delle comunicazioni di posta elettronica e, più specificamente, sul filtraggio delle comunicazioni in linea per la rimozione di virus, spam e contenuti illeciti.

4.2.5. Azioni proposte

La Commissione invita:

- le imprese a garantire che le informazioni comunemente fornite per l'acquisto di programmi software siano conformi alla normativa comunitaria in materia di protezione dei dati;

- le imprese a vietare per contratto l'utilizzo illegale del software nella pubblicità, a sorvegliare le modalità con cui le pubblicità raggiungono i consumatori e le pratiche scorrette;

- i fornitori di servizi di posta elettronica ad attuare politiche di filtraggio conformi alla raccomandazione e alle linee guida in materia di filtraggio della posta elettronica

4.3. Azione a livello europeo

La Commissione continuerà ad affrontare le questioni legate allo spam, ai programmi spia e ai software maligni nei consessi internazionali, negli incontri bilaterali e, ove appropriato,

---

33 http://www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf

34 Parere 2/2006, WP 118.

attraverso accordi con i paesi terzi e continuerà a promuovere la cooperazione tra i soggetti interessati, compresi gli Stati membri, le autorità competenti e le imprese del settore. Essa adotterà inoltre iniziative nel settore della legislazione e della ricerca finalizzate a imprimere un rinnovato impulso alla lotta contro le pratiche scorrette che minacciano la società dell'informazione. La Commissione è attualmente al lavoro sull'ulteriore elaborazione di una strategia coerente per la lotta contro la cybercriminalità, strategia che sarà presentata in una comunicazione che dovrebbe essere adottata all'inizio del 2007.

4.3.1. Riesame del quadro normativo

La comunicazione della Commissione[35] sul quadro normativo comune per le reti ed i servizi di comunicazione elettronica propone di rafforzare le norme nel settore della riservatezza e della sicurezza. In base alla proposta, gli operatori delle reti e i fornitori di servizi sarebbero obbligati a:

- informare l'autorità competente di uno Stato membro di ogni eventuale violazione di sicurezza che abbia portato alla perdita di dati personali e/o ad interruzioni nella continuità della fornitura del servizio;

- informare i loro clienti di ogni violazione di sicurezza che abbia comportato la perdita, la modifica, l'accesso o la distruzione di dati personali dei clienti.

Le autorità nazionali di regolamentazione avranno la facoltà di controllare che gli operatori mettano in atto politiche di sicurezza adeguate e potranno essere fissate nuove norme che prevedano **mezzi di ricorso specifici** oppure un'indicazione del **livello delle sanzioni** previsto per le violazioni.

4.3.2. Il ruolo dell'ENISA

Le proposte contengono inoltre una clausola che riconosce il ruolo consultivo dell'ENISA nelle questioni legate alla sicurezza. Gli altri compiti previsti per l'ENISA sono delineati nella comunicazione della Commissione sulla strategia per una società dell'informazione sicura[36] e comprendono:

- la creazione di un partenariato di fiducia tra gli Stati membri e le parti interessate al fine di sviluppare un **quadro adeguato per la raccolta di dati** sugli incidenti a danno della sicurezza e sulla fiducia dei consumatori.

L'ENISA coordinerà da vicino tale quadro insieme a Eurostat per quanto attiene alle statistiche comunitarie relative alla società dell'informazione e nell'ambito della valutazione comparativa i2010[37].

- l'esame della **possibilità di creare un sistema europeo di condivisione delle informazioni e di allerta** che permetta di rispondere efficacemente alle minacce esistenti ed emergenti alle reti elettroniche.

---

35 http://europa.eu.int/information_society/policy/ecomm/tomorrow/index_en.htm

36 *Supra* 1.

37 Quadro di valutazione comparativa del gruppo di alto livello i2010 del 20 aprile 2006.

4.3.3. Ricerca e sviluppo

Il prossimo programma quadro (PQ7) è finalizzato a proseguire lo sviluppo della conoscenza e delle tecnologie per rendere sicuri i servizi e i sistemi d'informazione in stretto coordinamento con le iniziative strategiche. I temi di lavoro collegati ai software maligni comprenderanno le botnet e i virus nascosti e gli attacchi contro i servizi mobili e vocali.

4.3.4. Cooperazione internazionale

Dato che internet è una rete globale, tutti si devono impegnare nella lotta contro lo spam, i programmi spia e i software maligni. La Commissione, pertanto, intende rafforzare il dialogo e la cooperazione con i paesi terzi nella lotta contro queste minacce in rete e contro le attività criminali ad esse legate. A tal fine, la Commissione cercherà di fare in modo che negli accordi tra l'UE e i paesi terzi si affronti la problematica dello spam, dei programmi spia e dei software maligni, cercherà di ottenere il deciso impegno dei paesi terzi più interessati a collaborare con gli Stati membri dell'UE per combattere tali minacce più efficacemente e seguirà da vicino l'applicazione degli obiettivi stabiliti di comune accordo.

4.3.5. Azioni proposte

La Commissione:

- proseguirà le azioni di sensibilizzazione e di promozione della cooperazione tra i soggetti interessati;

- continuerà a concludere accordi con i paesi terzi che comprendano la questione della lotta contro lo spam, i programmi spia e i software maligni;

- presenterà all'inizio del 2007 nuove proposte legislative che rafforzino le norme in materia di riservatezza e sicurezza nel settore delle comunicazioni e una strategia sulla cybercriminalità;

- attingerà all'esperienza dell'ENISA nelle questioni legate alla sicurezza;

- sosterrà la ricerca e lo sviluppo nell'ambito del PQ7.

5. CONCLUSIONI

Minacce in rete quali lo spam, i programmi spia e i software maligni compromettono la fiducia nella società dell'informazione e la sua sicurezza ed hanno ripercussioni finanziarie significative. Nonostante le iniziative di alcuni Stati membri, **le azioni** intraprese nell'Unione nel suo complesso **sono insufficienti ad affrontare tale problema**. La Commissione sta svolgendo un ruolo di intermediaria per sensibilizzare i soggetti interessati alla necessità di un maggiore impegno politico per la lotta contro queste minacce.

È necessario intensificare l'attività delle autorità competenti diretta a far osservare la legge in modo da colpire chiunque violi consapevolmente la legge. È necessario che anche il settore adotti misure a integrazione di quelle poste in essere dalle autorità. È necessaria una cooperazione a livello nazionale, sia all'interno del governo che tra il governo e le imprese del settore. La Commissione rafforzerà il dialogo e la cooperazione con i paesi terzi e studierà la possibilità di presentare nuove proposte legislative; avvierà

inoltre ricerche per rafforzare ulteriormente la riservatezza e la sicurezza nel settore delle comunicazioni elettroniche.

Un'attuazione integrata, e possibilmente coordinata, delle azioni descritte nella presente comunicazione può contribuire a ridurre le minacce in linea che compromettono l'economia e la società dell'informazione.
La Commissione sorveglierà l'attuazione di queste azioni e, entro il 2008, valuterà se siano necessarie ulteriori iniziative.