Elementi di Sicurezza Informatica
(A.A. 2009-2010)

SPAM

Cecilia Bracuto

26 Maggio 2010

Indice

1 Introduzione

Il termine *spam* trae origine da uno sketch comico del Monty Python's Flying Circus ambientato in un locale nel quale ogni pietanza proposta dalla cameriera era a base di Spam (un tipo di carne in scatola molto diffuso negli USA e prodotto da un'azienda di nome Hormel). Man mano che lo sketch avanza, l'insistenza della cameriera nel proporre piatti con "spam" ("uova e spam, uova pancetta e spam, salsicce e spam" e così via) si contrappone alla riluttanza del cliente per questo alimento, il tutto in un crescendo di un coro inneggiante allo "spam" da parte di alcuni Vichinghi seduti nel locale.
I Monty Python prendono in giro la carne in scatola Spam per l'assidua pubblicità che la marca era solita condurre.
L'idea che ha portato alla scelta del termine è quella di un disturbo che ostacola la possibilità di comunicare.
Lo spamming è l'invio di grandi quantità di messaggi indesiderati (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.
Nella terminologia informatica gli spam possono essere designati anche con il sintagma di *junk-mail*, che letteralmente significa posta-spazzatura, a rimarcare la sgradevolezza prodotta da tale molestia digitale.
Il principale scopo dello spamming è la pubblicità, il cui oggetto può andare dalle più comuni offerte commerciali a proposte di vendita di materiale pornografico o illegale, come software pirata e farmaci senza prescrizione medica, da discutibili progetti finanziari a veri e propri tentativi di truffa. Siccome lo spam è economico da inviare, un ristretto numero di persone che lo inviano può saturare Internet con i propri messaggi. Nonostante solo un piccolo numero dei destinatari sia intenzionato a comprare i prodotti proposti, ciò consente di mantenere questa pratica attiva. Un'altra porzione di messaggi non richiesti è anche di carattere non commerciale; alcuni esempi comprendono i messaggi di propaganda politica e le catene di Sant'Antonio.
I messaggi vengono, in sostanza, diffusi avvalendosi delle funzionalità della rete, senza rispettare lo scopo per il quale tali funzionalità esistono. Facciamo un esempio banale: il campanello di casa vostra serve per avvertirvi dell'arrivo di un visitatore, del postino e così via; non l'avete installato perché i ragazzini possano divertirsi. Quello che suona il campanello e se la dà a gambe commette quindi un abuso. L'analogia con quanto avviene in rete non si può spingere tanto più in là, ma il concetto base per capire lo spam è esattamente questo. Per definizione lo spam viene inviato senza il permesso del destinatario ed è un comportamento ampiamente considerato inaccettabile dagli *Internet Service Provider (ISP)* e dalla maggior parte degli utenti di Internet. Mentre questi ultimi trovano lo spam fastidioso e con contenuti spesso offensivi, gli ISP vi si oppongono anche per i costi del traffico generato dall'invio indiscriminato. Ci sono però anche ISP consenzienti i quali mettono a disposizione i loro server per l'invio di e-mail di spam dietro pagamento. Tuttavia l'ISP potrebbe non essere consenziente ma, un po' per indolenza e un po' per necessità, non intervengono in maniera decisa in quanto lo spam è una fonte di guadagno per quegli ISP che vendono soluzioni antispam.
Sondaggi hanno indicato che al giorno d'oggi lo spam è considerato uno dei maggiori fastidi di Internet; l'invio di questi messaggi costituisce una violazione del contratto *Acceptable Use Policy* (condotta d'uso accettabile) di molti ISP e pertanto può portare all'interruzione dell'abbonamento (account) del mittente.
Quale tipo di attività costituisca spamming è materia di dibattiti, e le definizioni divergono in base allo scopo per il quale è definito, oltre che dalle diverse legislazioni. Lo spamming è

considerato un reato in vari paesi e in Italia l'invio di messaggi non sollecitati è soggetto a sanzioni.

2 Come funziona la posta elettronica

Simple Mail Transfer Protocol (SMTP) è il protocollo standard per la trasmissione via internet di e-mail. È un protocollo relativamente semplice, testuale, nel quale vengono specificati uno o più destinatari di un messaggio, verificata la loro esistenza per poi trasferire il messaggio. Il protocollo SMTP utilizza come protocollo di livello transport TCP. Il client apre una sessione TCP verso il server sulla porta 25.
SMTP è un protocollo che permette soltanto di inviare messaggi di posta, ma non di richiederli ad un server: per fare questo il client di posta deve usare altri protocolli, quali il POP3 (Post Office Protocol) e l'IMAP (Internet Message Access Protocol).

3 Come opera uno spammer

Uno *spammer*, cioè l'individuo autore dei messaggi spam, invia messaggi identici (o con qualche personalizzazione) a migliaia di indirizzi e-mail. Questi indirizzi possono essere:

- ottenuti in maniera automatica dalla rete (articoli di Usenet, pagine web) mediante appositi programmi;
- acquistati direttamente dagli ISP;
- indovinati usando liste di nomi comuni;
- ottenuti utilizzando i programmi chiamati spider. Lo spider (o ragno) è un piccolo software utilizzato da un motore di ricerca per esplorare il web. Quando lo spider si imbatte in un nuovo sito, memorizza il contenuto delle varie pagine e cataloga i link che puntano in direzione di altri siti. Seguendo questi link lo spider continua il suo percorso dirigendosi verso altri siti.
  Questa è una tecnica ormai discretamente diffusa con cui gli spammer si procurano indirizzi e-mail. Attacchi di questo genere vengono chiamati *dictionary attack*: lo spammer genera un numero di indirizzi che potrebbero esistere, come adam@aol.com che, se esistesse, riceverebbe molto spam.

4 Tipi di spamming

Non esiste un solo metodo per inviare spam.

- **Spamming attraverso e-mail diretta.** Questo metodo si basa sul fatto che molti spammer mandano i messaggi attraverso gli *open mail relay*. I server SMTP, usati per inviare e-mail attraverso Internet, inoltrano la posta da un server a un altro; i server utilizzati dagli ISP richiedono una qualche forma di autenticazione che garantisca che l'utente sia un cliente dell'ISP. Però i server open relay non controllano correttamente chi sta usando il server e inviano tutta la posta al server di destinazione, rendendo più difficile rintracciare lo spammer.

I più grandi ISP riferiscono che lo spam consuma la capacità dei loro server di posta elettronica in quantità che varia da un terzo a due terzi. Molti considerano lo spam come una forma di furto di servizi.

- **Spamming per interposta persona.** Questo metodo è un mezzo subdolo utilizzato sfruttando l'ingenuità di molta gente. Per l'esattezza si intende l'invio di e-mail commerciali ad alcuni destinatari, conosciuti e magari regolarmente iscritti ad una newsletter dello spammer, invitandoli a far conoscere una certa promozione ad uno o più persone conosciute dall'ingenuo destinatario, invogliandolo talvolta con qualche piccolo compenso. Grazie a questo sistema sarà l'ingenuo destinatario a spammare altre caselle di posta di suoi conoscenti coprendo colui che c'è dietro e che guadagnerà da questo comportamento.

5 Come difendersi

Esistono diversi servizi e software, spesso chiamati *antispam*, che i server e-mail e gli utenti possono utilizzare per ridurre il carico di spam sui loro sistemi e sulle loro caselle di posta. Riportiamo alcune tecniche utilizzate da questi software:

- **Bloccaggio.** Questa tecnica si basa sul rifiuto dei messaggi provenienti dai server conosciuti come spammer. Il lavoro viene fatto sul server man mano che i messaggi arrivano, senza il bisogno che il client sia connesso alla rete. Quando il client si connette trova i soli messaggi accettati, senza quindi perdere tempo con gli altri. Sicuramente essa riduce l'ammontare di spam inviato alle caselle postali degli utenti ma permette anche di ridurre la banda sprecata, rifiutando i messaggi prima che siano trasmessi al server dell'utente.
  Una specifica tecnica di bloccaggio comprende le *DNSBL (DNS-black lists)*, che sono elenchi di indirizzi IP selezionati secondo linee guida specifiche di ciascuna lista. Tali liste vengono mantenute attuali nel tempo (gli indirizzi o blocchi di indirizzi che le compongono vengono aggiunti o tolti quando necessario) e messe a disposizione di chiunque desideri consultarle. La ragione per cui è così comune la pratica di catalogare gli indirizzi IP tramite queste liste è che, in generale, ogni indirizzo IP che emette posta tende ad essere sorgente o solo di spam o solo di posta legittima. Esistono anche sorgenti miste (e gli spammer cercano, in effetti, di battere anche questa strada), però esistono certamente tantissimi IP che sono sorgenti di solo spam. Se qualcuno mantenesse una tale lista e riuscisse ad aggiornarla in continuazione in modo che, idealmente, la lista contenesse tutti e soli gli indirizzi IP dai quali proviene spam, ecco che ne potrebbe trarre beneficio anche chi non avesse le risorse, le informazioni o l'esperienza necessarie per crearsi in proprio una tale lista. Ogni lista è gestita da chi ha deciso di crearla e di mantenerla su un proprio sistema. Normalmente, chi cerca una lista di cui potersi davvero fidare al fine di bloccare le e-mail in arrivo, farebbe bene a considerare importante che siano soddisfatti questi due requisiti: sia noto il modo in cui vengono decisi gli inserimenti e le rimozioni di indirizzi dalla lista; deve trattarsi di modalità che l'utilizzatore della lista abbia ben capito e che ritenga valide e appropriate per le proprie esigenze. In effetti, le blacklist più diffuse e attendibili soddisfano a tali caratteristiche. Questo metodo permette ad un server di posta di essere facilmente impostato per rifiutare la posta che proviene da questi indirizzi. Ci sono diverse liste di DNSBL, che hanno politiche diverse: alcune liste contengono server che emettono spam, altre contengono open mail relay, altre elencano gli ISP che supportano lo spam.

- **Filtraggio.** Per filtri si intendendo delle "regole", da verificarsi sul testo delle email in arrivo una volta che siano state ricevute. A seconda che ciascuna regola risulti verificata o no, si otterrà un differente trattamento del messaggio. Un esempio tipico potrebbe essere di questo genere: se il titolo dell'e-mail contiene la parola "sexy" allora cancella il messaggio. In questo caso occorre un certo qual traffico lungo la connessione e, soprattutto, del tempo trascorso on-line mentre il programma opera. Inoltre, quando si elimina un messaggio, quel messaggio ha già costituito un costo per il provider (che ha dovuto usare banda per farlo arrivare, spazio disco per memorizzarlo e risorse di macchina per elaborarlo). Quindi il vantaggio di questo approccio è decisamente limitato.
  I software che utilizzano questa tecnica analizzano in modo automatico il contenuto dei messaggi e-mail ed eliminano o spostano in una cartella speciale quelli che somigliano a spam. Sicuramente anche il filtraggio, come il bloccaggio, riduce l'ammontare di spam inviato alle caselle postali degli utenti ma tende ad essere una soluzione più accurata, poiché può esaminare tutti i dettagli del messaggio.
  Fino a poco tempo fa, le tecniche di filtraggio facevano affidamento sugli amministratori di sistema che specificavano le liste di parole o espressioni regolari non permesse nei messaggi di posta. L'amministratore poteva inserire queste parole nella configurazione del filtro. Se il messaggio in arrivo conteneva una di quelle parole presenti nell'elenco creato, il server avrebbe scartato il messaggio. Essa è una tecnica vantaggiosa in quanto facile da implementare. D'altro canto lo svantaggio di questo *filtraggio statico* consiste nella difficoltà di aggiornamento e nella tendenza ai falsi positivi (e-mail regolari scambiate erroneamente come spam): è sempre possibile che un messaggio non-spam contenga quella frase o parola nell'elenco.
  Sono stati quindi introdotti altri tipi di filtraggio:

  - *filtraggio euristico.* Esso si basa nell'assegnare un punteggio numerico a frasi o modelli che si presentano nel messaggio. Quest'ultimo può essere positivo, indicando che probabilmente contiene spam o negativo in caso contrario. Ogni messaggio è analizzato e viene annotato il relativo punteggio, esso viene in seguito rifiutato o segnalato come spam se quest'ultimo è superiore ad un valore fissato. In ogni caso, il compito di mantenere e generare le liste di punteggi è lasciato all'amministratore.
  - *filtraggio statistico.* Questo metodo, proposto per la prima volta nel 1998 e reso popolare da un articolo di Paul Graham nel 2002, usa metodi probabilistici, ottenuti grazie al Teorema di Bayes, per predire se un messaggio è spam o no, basandosi su raccolte di email ricevute dagli utenti.

- **Tecniche miste.** Da qualche tempo stanno crescendo vari sistemi di filtraggio che uniscono più tecniche di riconoscimento dello spam, in modo da minimizzare il rischio di falsi positivi e aumentare l'efficienza del filtraggio. Si può quindi pensare di combinare il bloccaggio per DNSBL con il filtraggio euristico e statistico, come alcuni programmi iniziano a prevedere, e fare così in modo di unire i pregi di ogni metodo di filtraggio e contemporaneamente ridurre i rischi grazie ai controlli multipli.

6 Come comportarsi

Oltre all'installazione di software di filtraggio e bloccaggio, gli utenti possono proteggersi dall'attacco dello spam in molti altri modi.

- **Tenere poco esposto il proprio indirizzo di e-mail.** Un modo con cui gli spammer ottengono gli indirizzi e-mail è il setaccio del Web e di Usenet per stringhe di testo che assomigliano a indirizzi. L'indirizzo e-mail va reso pubblico con molta cautela. Una volta che un indirizzo di e-mail finisce nelle mani degli spammer, non c'è più niente da fare: verrà venduto ad altri, poi ad altri ancora. Perciò se l'indirizzo di una persona non è mai apparso in questi posti, non potrà essere trovato. Un sistema per evitare questa raccolta di indirizzi è falsificare i nomi e indirizzi di posta. E' preferibile non mettere l'indirizzo negli appositi campi, oppure metterlo con alterazioni.
  In base agli standard di rete codificati nelle RFC, l'indirizzo sarebbe da mettere senza alterazioni. Per questa ragione molti non adottano questa soluzione e, prevedibilmente, considerano con scarsa simpatia coloro che la praticano. Un'alternativa frequentemente suggerita è l'adozione di indirizzi "a perdere", che vengono adoperati solamente per postare sui newsgroup e vengono chiusi in breve tempo, non appena inizino a ricevere spam.
  Se si intende comunque mettere nei post su Usenet un indirizzo alterato o non valido, è importante che almeno si seguano alcune avvertenze: è opportuno adottare un'alterazione che renda l'indirizzo non valido del tutto. Preferibilmente è meglio fare in modo che la parte dopo la @ diventi un riferimento non valido. Vedendo l'indirizzo, l'alterazione deve essere il più possibile evidente. Ciò che potrebbe dare il massimo fastidio a chi, vedendo l'indirizzo apparentemente valido, desiderasse scrivergli, sarebbe usarlo, e poi accorgersi che il messaggio è fallito. Sostituire semplicemente un carattere con un altro (anche se si tratta di caratteri speciali) non va bene poiché l'alterazione, anche se per chi ha apportato la modifica è ovvia, non è evidente per altri. Nel corpo del messaggio (per esempio nella signature) è opportuno inserire indicazioni che consentano, ad un lettore interessato, di ricavare l'effettivo indirizzo.
  Quindi gli utenti che vogliono ricevere in modo legittimo posta riguardante il proprio sito Web o i propri articoli di Usenet possono alterare i loro indirizzi in modo tale che gli esseri umani possano riconoscerli ma i software degli spammer no.
  Per esempio,

  mariorossi@abcd.it

  può diventare

  mariorossi@abcdNOSPAM.it

  oppure

  mariorossi@TOGLIMIabcd.it.

  Questo sistema è detto **address munging**, dalla parola munge che significa rompere. E' stato però riportato che alcuni programmi di estrazione indirizzi dai newsgroup vantano, tra le proprie funzionalità, la ricerca ed eliminazione delle più comuni di queste stringhe (come NOSPAM o REMOVETHIS). Occorre quindi essere creativi e cambiare strategia di tanto in tanto. Originale la trovata di colui che ha messo: "Per mandarmi e-mail togliere LEDITADALNASO".
  Anche se l'indirizzo non viene mai reso pubblico, ha ugualmente una buona probabilità di comparire prima o poi negli elenchi degli spammer a causa dei dictionary attack.

- **Utilizzare indirizzi non troppo brevi.** Uno spammer ostinato può sempre ricavare a mano l'indirizzo. Si tratta tuttavia di casi rari, in quanto un'attività di spam massivo ha bisogno di essere effettuata con strumenti automatici. Con questo tipo di attacchi, i dictionary attack, si cerca di scoprire nuovi indirizzi componendoli, per la parte alla destra della @, con nomi dominio validi e usando, per la parte alla sinistra della @, delle stringhe indovinate in base ad una qualche logica. Si può pensare che abbiano iniziato provando con stringhe come "john", "mary", "jsmith", "sales", "info" e simili, per sofisticare e automatizzare nel tempo la generazione. Da questi attacchi è possibile difendersi scegliendo indirizzi non troppo brevi.

- **Evitare di rispondere.** Se lo spammer riceve un'e-mail di risposta (che sia di protesta o, ancora più ingenuamente, di garbato rifiuto dell'offerta prospettata), questo ha per lui un unico valore: gli conferma che l'indirizzo di e-mail è valido e che, ad esso, corrisponde una persona che ne legge i messaggi. E' quindi probabile che inserisca l'indirizzo in altre liste o, come generalmente avviene, che rivenda l'indirizzo di e-mail ad altri spammer (un indirizzo la cui validità sia verificata ha un valore commerciale maggiore).

- **Non seguire istruzioni date nel messaggio.** Molti messaggi di spam contengono indirizzi o link ai quali viene indirizzato il destinatario. E' stato verificato che questi collegamenti comportano uno spam ancora maggiore. Se poi si trattasse di un messaggio formattato in HTML, non bisogna cliccare nulla di ciò che ci si vede sopra. Anzi, sarebbe meglio addirittura evitare di aprirlo nel browser. Un caso particolare che si verifica abbastanza spesso è quando lo spammer fornisce istruzioni per farsi togliere dai suoi elenchi. Vediamo un esempio:

  > We apologize for the intrusion.
  > To remove your name from our list reply
  > and type remove in the subject heading.

  Chi ci garantisce che una richiesta di remove venga onorata come promesso? Nessuno; anzi, in molti casi c'è addirittura evidenza del contrario, ossia chi invia la richiesta di remove viene di solito inserito in altri elenchi.

- **Non attuare forme di ritorsione diretta sullo spammer.** Effettuare ad esempio il *mailbombing* (letteralmente bombardamento postale), che è una forma di attacco informatico in cui grandi quantitativi di e-mail vengono inviati ad un unico destinatario provocandone l'intasamento della casella di posta, sarebbe un modo sicuro per passare dalla parte del torto. Azioni del genere potrebbero danneggiare, più ancora dello spammer, altri sistemi utilizzati da parecchi utenti che non c'entrano nulla. Gli amministratori di tali sistemi prenderebbero dei provvedimenti nei confronti di chi avesse perpetrato tale azione, il quale non avrebbe nessuna giustificazione valida.

- **Denunciare spam.** Abbiamo visto finora una serie di cose da non fare. Ora vediamo qual è l'unico provvedimento che può rivelarsi efficace. Esiste una sola cosa che possa mettere lo spammer in condizione di non poter più nuocere: perdere l'uso delle risorse che gli danno una presenza in rete. La maggioranza degli ISP proibisce esplicitamente ai propri utenti di fare spam e in caso di violazione essi vengono espulsi dai loro servizi. Rintracciare l'ISP di uno spammer e denunciarlo spesso porta alla chiusura dell'abbonamento.

Se il suo provider gli cancella improvvisamente l'abbonamento, lo spammer cercherà di attivarne un altro presso un altro provider. Fino a quel momento non potrà che rimanere fermo con il suo discutibile lavoro, così la nostra mailbox avrà finalmente un po' di giorni di tranquillità. Eventualmente, dopo aver trovato un altro provider lo spammer non potrà non chiedersi se vale la pena di farsi cacciare via anche da lì. Dover cambiare provider ogni qualche giorno è indubbiamente snervante. Ovviamente questo provvedimento può essere preso solo da chi fornisce allo spammer la connettività in rete, vale a dire dal suo provider. È quindi al suo provider che bisogna rivolgersi, cosa che si fa via e-mail. Occorre ovviamente individuare, per prima cosa, chi sia il provider dello spammer. Poi si cercherà di sapere qualcosa in più sul provider in questione, in particolare l'esatto indirizzo di e-mail a cui è previsto siano da inviarsi questo genere di segnalazioni. A questo punto si deciderà come scrivere l'e-mail.
Ma ne vale veramente la pena? Sì, perchè se nessuno mandasse le segnalazioni, i provider non avrebbero alcun mezzo per far rispettare i propri regolamenti d'uso del servizio, e neppure di rendersi conto tempestivamente dell'esistenza del problema. Gli spammer dilagherebbero e, di conseguenza, il volume di messaggi commerciali indesiderati esploderebbe, travolgendo la maggior parte delle infrastrutture di rete e dei server. La posta elettronica diventerebbe ben presto inservibile come mezzo di comunicazione. Passando poi al punto di vista più individuale-utilitaristico, se appare che uno spammer possiede il vostro indirizzo di e-mail, lasciarlo operare indisturbato è ovviamente solo a vostro svantaggio.
Il metodo più efficace per fermare gli spammer è di sporgere reclamo alle autorità competenti. Ciò impegna più tempo e impegno, però gli spammer vengono perseguitati legalmente e devono pagare multe e risarcimenti. In questo modo si annulla il vantaggio economico e l'attività può tradursi in una perdita economica.
Reclamare quando si riceve spam è la soluzione più diffusa, praticata da tantissime persone in tutto il mondo. Quando si reclama contro un messaggio di spam, è molto probabile che ci si trovi in compagnia di molti altri utenti che abbiano ricevuto lo stesso spam e, a loro volta, abbiano reclamato. Agendo incautamente si può al massimo rischiare di ricevere più spam: comunque, l'unico caso in cui questo rischio esiste è quando lo spammer è il provider di se stesso e, quindi, è proprio lui a ricevere il reclamo.

7 Normativa

La disciplina italiana concernente l'invio di posta elettronica a fini commerciali è disciplinata dall'art. 130 Codice Privacy. L'ambito di applicazione di detto articolo è proprio quello dello spamming, seppur la rubrica si limiti a parlare di comunicazioni indesiderate e non menzioni quelle semplicemente non richieste. Il modello di regolazione scelto dal legislatore italiano (e in generale da tutti gli stati aderenti alla Comunità Europea) è quello dell'"opt-in", che prevede la possibilità di avvalersi del trattamento dei dati personali solo dopo aver ottenuto il consenso del soggetto interessato. È inoltre vietato, sempre dall'art. 130 Codice Privacy, l'invio di comunicazioni a scopi pubblicitari, per la vendita diretta o per ricerche di mercato effettuate camuffando o celando l'identità del mittente o ancora senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i propri diritti. È però prevista una deroga ai dettami di tale articolo, che consente di utilizzare le coordinate di posta elettronica, fornite dall'interessato nel contesto della vendita di un prodotto o servizio, per l'invio di ulteriori messaggi promozionali

aventi ad oggetto simili beni o servizi, senza dover nuovamente chiederne il consenso.
Vi è poi nel nostro ordinamento un'ulteriore diposizione al riguardo, rinvenibile nel d.lgs. 9 aprile 2003, n.70 sul commercio elettronico. L'art. 9 afferma infatti che le comunicazioni commerciali non sollecitate, trasmesse da un prestatore per posta elettronica devono, in modo chiaro ed inequivocabile, essere identificate come tali fin dal momento in cui il destinatario le riceve e devono altresì contenere l'indicazione che il destinatario del messaggio può opporsi al ricevimento in futuro di tali comunicazioni.
Va da ultimo esaminato l'impianto sanzionatorio previsto dal nostro ordinamento. Anzitutto lo stesso art. 130 comma 6 attribuisce al Garante per la protezione dei dati personali, in caso di reiterata violazione delle disposizioni previste in tale ambito, il potere di provvedere, negli ambiti di un procedimento di reclamo attivato, tramite prescrizione ai fornitori di servizi di comunicazione elettronica (ISP), adottando misure di filtraggio o altre misure praticabili nei confronti di un certo indirizzo di posta elettronica.
Di ben maggiore deterrenza appare poi l'art. 167 del Codice Privacy, nel quale si prevede che, salvo il fatto non costituisca più grave reato, chiunque proceda al trattamento dei dati personali in violazione di quanto previsto nel Codice stesso, al fine di trarne un profitto o recare ad altri un danno, è punito con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione di tali dati, con la reclusione da sei a ventiquattro mesi. Al p.to 2 inoltre si prevede che chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.
L'attività di spamming espone, infine, ai sensi dell'art. 161 Codice Privacy, alla sanzione amministrativa di omessa informativa (di cui all'art 13), la quale va da un minimo di seimila euro ad un massimo di trentaseimila euro. La sanzione viene erogata dall'autorità Garante per la protezione dei dati personali a seguito di un apposito ricorso ai sensi degli artt. 145 ss. Codice Privacy; il medesimo ricorso non può essere riproposto se è già stata adita l'autorità giudiziaria.
La prima controversia italiana avente ad oggetto attività di spamming è stata risolta dal Giudice di Pace di Napoli, che, con sentenza 26 giugno 2004, ha riconosciuto l'illiceità di tale attività, condannando il titolare del trattamento al risarcimento del danno patrimoniale, non patrimoniale, esistenziale e da stress subito dal titolare della casella di posta elettronica. L'assetto che deriva dalle regole appena esposte, in piena coerenza con la vigente disciplina nazionale sulla data protection, qualifica dunque il nostro come un sistema improntato al cosiddetto "opt-in" (necessità del consenso preventivo), salvo il temperamento relativo alla comunicazione via e-mail finalizzata alla vendita di "propri prodotti o servizi analoghi". Circa il rapporto tra il consenso richiesto dalla normativa privacy e quello imposto dall'art. 58, comma 1, del Codice del consumo, pur essendo ancora oggi il tema fortemente dibattuto, restano fermi però alcuni punti di riferimento che devono costituire i criteri guida per la soluzione di questo problema:

- si tratta di due consensi aventi natura diversa, per il semplice fatto che tutelano interessi diversi (quello alla riservatezza da un lato, e quello alla correttezza del comportamento del professionista dall'altro);

- comuni sono le sanzioni che derivano dalla violazione delle norme.

Si deve comunque sottolineare che in questo tema e in virtù di quanto prima sostenuto in tema di sanzioni debba ritenersi più significativo l'orientamento del Garante Privacy il quale, in numerosi provvedimenti, ha dichiarato l'illegittimità di qualsiasi comunicazione non preventivamente autorizzata: rilevato che ai sensi dell'art. 130 del Codice (salvo quanto previsto dal

comma 4 del medesimo articolo) il consenso preventivo degli interessati è richiesto anche per l'invio di una sola comunicazione mediante posta elettronica volta ad ottenere il consenso per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale o, comunque, per fini promozionali.