Il fenomeno del Cyberstalking

Analisi del fenomeno delle molestie via Internet e della risposta del legislatore

Massimo Messina
Università degli Studi di Urbino, Facoltà di Sociologia
Dottorando di ricerca in Sociologia dei fenomeni culturali e dei processi normativi

Maggio 2005

Abstract

Internet rappresenta un'opportunità anche per quanto riguarda le azioni delittuose. Da una parte gli attori criminali utilizzano la rete come strumento di efficienza, dall'altra Internet favorisce la nascita di nuovi crimini che sono significati solo all'interno della rete stessa. La situazione, oramai evidente anche in Italia, porta non solo ad una revisione critica delle norme di Diritto Penale e di Procedura Penale, ma anche alla necessità di innovare le metodologie su cui si basavano le tradizionali indagini investigative. Questi fenomeni criminali, oltre ad essere "virtuali" sono connotati da una rapidità e da una trans-nazionalità che impone nuovi rapporti tra gli Stati e le loro polizie. Di questi fenomeni, quello delle minacce e molestie via rete (il Cyberstalking) appare trascurato in termini di ricerca, di tutela e di corpo normativo.
Questo lavoro vuole esplorare il fenomeno, evidenziando le criticità attuali, e proponendo spunti per eventuali ricerche successive che consentano di approfondire meglio i punti evidenziati.

Introduzione

Internet ed il Cyberspace sono sicuramente veicoli di progresso, ma allo stesso tempo, con la facilità di accesso, l'economicità, e soprattutto l'anonimato, rappresentano un'attrazione per quanti professano attività fraudolente, creando nuove fattispecie criminose e variazioni di quelle tradizionali.

Infatti il crimine professionale cerca efficentamenti per le proprie azioni ed alcune di queste si prestano ad essere innovate tramite l'information technology: furti di informazioni e spionaggio, truffe e frodi, gioco d'azzardo, prostituzione, traffici vari (armi, droga, organi), molestie e minacce, pedofilia, riciclaggio, terrorismo e sette sataniche[1].
Allo stesso tempo, si sono sviluppate delle forme di crimine nuove e peculiari alla rete: Cyberpedofilia, Cyberterrorismo, hacking, virus, spamming, violazione della privacy, on-line gambling, diffusione di informazioni illegali e net-strike[2].

[1] Marco Strano, "Nuove tecnologie e nuove forme criminali", 2002, Cybercrime International Conference, ottenibile da http ://www.poliziadistato . it/pds/primapagina/cybercrime/index.html copia del 10-05-2005
[2] Ibidem nota 1

L'attenzione data dai media ad alcuni di questi fenomeni delittuosi ha generato un allarme-politico istituzionale che ha consentito la produzione di un corpo normativo specifico, la cui efficacia e completezza dipende grandemente dal crimine e dalla nazione a cui ci si riferisce.

Spesso questo corpo normativo traduce un'esigenza di trasformazione del Cyberspace in un luogo in cui applicare le norme della proprietà privata e della protezione degli investimenti e degli interessi economici, tralasciando di regolamentare aspetti più propriamente legati alla tutela della persona (se si fa l'eccezione della protezione dei minori); tra questi reati c'è la minaccia e la molestia on-line.

Negli USA il comportamento di minaccia o molestia perpetuato da una persona in modo ripetuto e continuato è indicato con il termine ***Stalking***. Esempi di questo comportamento sono il seguire una persona a distanza, mostrarsi non invitato a casa o sul luogo di lavoro della vittima, fare delle telefonate di molestia, lasciare oggetti o messaggi scritti non richiesti e in modo continuato, e compiere atti vandalici sulla proprietà della vittima.
L'attività di molestare qualcuno, in modo anonimo, con strumenti informatici od altre apparecchiature elettroniche e' detto ***Cyberstalking***.

Anche se le minacce e le molestie on-line possono presentarsi in varie modalità, esse non sono molto diverse da quelle che avvengono nella vita reale.
Il Cyberstalker, al fine di perpetuare il proprio crimine, si avvale di mezzi informatici contro i quali i sistemi di protezione "fisici" risultano inutili. L'idea di poter contare su un anonimato pressoché completo (idea che il più delle volte si rivela totalmente sbagliata), unita ai particolari mezzi di interazione, provoca dei comportamenti che rendono anche i classici sistemi di controllo sociale della devianza totalmente inefficaci.

La natura e l'estensione del fenomeno del Cyberstalking sono difficili da quantificare, ma indipendentemente dalla situazione attuale, tutto lascia supporre che il Cyberstalking crescerà di impatto via via che Internet affonderà meglio le radici nel tessuto più profondo della nostra società. Anche se le polizie postali (cioè le polizie che per competenza si occupano di crimini legati alle telecomunicazioni) e le istituzioni responsabili di legiferare e vigilare su questo fenomeno diventano sempre più attive, esse sono molte volte impreparate sia a capire il fenomeno, sia a combatterlo. Allo stesso modo alcuni Internet Service Providers (ISPs) stanno attivamente contrastando il Cyberstalking, inserendo nelle loro pagine WEB strumenti di denuncia che, insieme alle organizzazioni senza scopo di lucro che sono state create in questi anni, costituiscono un sistema normativo alternativo rispetto a quello del diritto positivo interno al Cyberspace.

L'idea dietro questo lavoro è quella di esplorare il fenomeno del Cyberstalking identificando possibili spunti di ricerca inquadrabili a livello disciplinare all'interno della sociologia del diritto, od altri più indirizzabili in termini culturali e della devianza, che possano essere successivamente sviluppati.
Per questo, oltre a definire i confini del Cyberstalking e capire quali molestie perpetuate nel Cyberspace possano effettivamente essere considerate alla stregua di reati, si affronterà la differenza di interpretazione tra le molestie nella vita reale e quelle nel Cyberspace. Sarà anche analizzata la controversa questione del test della vera minaccia (*true threat) e* cioè cosa un sospetto molestatore deve aver fatto perchè una persona ragionevole possa dimostrare di essere stata angosciata dalle minacce ricevute.

Non avendo ancora rilevanza nel nostro Paese, si e' analizzato il fenomeno dal punto di vista del legislatore e dagli istituti di controllo degli Stati Uniti d'America, nazione che certamente sta vivendo il Cyberstalking con maggiore impatto rispetto ad altri a causa della diversa maturità della rete Internet[3], descrivendo comunque cosa è stato fatto sino ad oggi in Italia per reati simili (es Pedofilia via rete).

Prendendo spunto da un rapporto preparato dall'allora Ministro della Giustizia degli Stati Uniti (*Attorney General) Janet Reno,* per il Vice Presidente *Al Gore*, si vedranno anche quali potranno essere le possibili evoluzioni legislative nei prossimi anni.

In questa esplorazione, per mancanza di spazio, si è volutamente esclusa la componente "professionale" del fenomeno e cioè quella che riguarda le minacce, le aggressioni, le frodi e le attività di mobbing effettuate all'interno del mondo del lavoro attraverso strumenti elettronici.

Cosa è il Cyberstalking

Al momento non c'è una definizione universalmente accettata di Cyberstalking[4] e le varie informazioni ottenibili tramite Internet sono molte volte disperse e non riassunte in un'unica definizione. Di seguito si tenterà di trovare una definizione del fenomeno, che prenda in considerazione sia quelle prelevate da Internet (importanti in quanto ci consentono di avere anche un'idea dell'auto-percezione dei gruppi sociali che fanno intenso utilizzo di internet rispetto ai propri comportamenti) sia le definizioni che è possibile dedurre dalle ormai numerose leggi emanate negli Stati Uniti (paese che già da tempo ha riconosciuto il fenomeno e sta tentando di controllarlo).

L'ex Ministro della Giustizia USA Janet Reno, in un suo rapporto[5] dell'Agosto 1999, definisce il Cyberstalker come un molestatore informatico che usa la posta elettronica o qualsiasi altro mezzo digitale per molestare ripetutamente e perseguitare un'altra persona.

L'azione di molestare attraverso mezzi di comunicazione e' stata definita in vario modo nei vari Stati Americani; vediamone alcuni esempi:

> **Alabama**[6]: presenta una definizione molto semplice indicando come crimine telematico l'intento di molestare od allarmare un'altra persona utilizzando mezzi di comunicazione, e indicando chiaramente l'importanza che l'anonimato ha per ritenere il caso un reato telematico. I mezzi utilizzati sono indicati in modo generico quali: telefono, telegrafo, posta o altra forma di comunicazione scritta od elettronica. L'azione criminale viene identificata nella creazione di situazioni che causano nella vittima un'apprensione per la propria incolumità.

---

[3] Si vedano i rapporti di penetrazione di Internet rispetto alla popolazione illustrati nel paragrafo "I numeri del Cyberstalking"

[4] "What Is Cyberstalking? From the U.S. Department of Justice", CyberGuards, ottenibile da http://www.cyberguards.com/CyberStalking.html, referenza acceduta il 30/04/2005

[5] 1999 Report on Cyberstalking: a New Challenge for Law Enforcement and Industry; A Report from the Attorney General to the Vice President Al Gore, disponibile su http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm, pagina acceduta il 24/04/2005.

[6] http://www.haltabuse.org/resources/laws/index.shtml, acceduta il 12-05-2005

Massachusetts[7] : A differenza dell'Alabama, viene indicato un crimine di molestia generico estendendo l'inclusione anche ad atti, azioni o minacce fatte attraverso posta o attraverso l'uso di apparecchiature telefoniche o tele-comunicative includendo, ma non limitate a, posta elettronica, comunicazioni Internet e comunicazioni simili. Un'altra differenza dall'impostazione precedente e' che viene ignorata la componente di anonimicità dell'attacco ma si fa particolare attenzione all'intenzione di dolo ed all'aspetto temporale durante la quale la minaccia avviene. Per esserci azione criminale, il persecutore deve mostrare volontà di dolo in modo continuato per un periodo di tempo. Il danno viene di nuovo identificato con la creazione di una situazione di tensione emotiva nella vittima preoccupata per la propria incolumità, ma viene anche introdotto il problema di quale sia la soglia corretta di percezione della situazione di allarme; la persona che si allarma deve essere in piena facoltà mentale e deve dimostrare di soffrire di consistenti angosce emotive. Questa angoscia viene chiaramente indicata come il risultato di una minaccia del persecutore con l'intento di incutere nella vittima la paura di essere uccisa o di essere ferita.

North Carolina[8] : la legislazione del North Carolina in proposito può essere considerata un'evoluzione dei due riferimenti legislativi presi in esame precedentemente in quanto è una descrizione completa del fenomeno del Cyberstalking, ed e' ad esso specificatamente riferito. Vengono anche dettagliati i significati di Comunicazione Elettronica e di Posta Elettronica:

1. Comunicazione Elettronica: qualunque trasferimento di segni, segnali, scritture, immagini, suoni, dati o informazioni di qualsiasi natura, trasmessa interamente o in parte attraverso filo, radio, computer, elettromagneti, fotoelettriche o sistemi foto ottici.
2. Posta Elettronica: la trasmissione di informazioni o comunicazioni (attraverso l'uso di Internet, un computer, un FAX, un pager, un telefono cellulare, un video registratore o altri oggetti elettronici) inviate ad una persona identificata da un unico indirizzo e ricevute da quella persona

L'azione illegale viene articolata su quattro punti:

- L'uso in posta elettronica o in comunicazioni elettroniche di qualsiasi parola o linguaggio che minaccino di infliggere dolore fisico a qualche persona o al figlio di questa persona, sorella, sposo/a o dipendente, o di minacciare di danneggiare la proprietà , o per lo scopo di estorcere denaro o altre cose di valore.
- Inviare per posta elettronica, o comunicare elettronicamente ad un altro, in modo ripetitivo, in seguito o no a conversazione, con lo scopo di abusare, dare fastidio, minacciare, terrorizzare, molestare o imbarazzare qualsiasi persona.
- Inviare per posta elettronica, o comunicare elettronicamente ad un altro, in modo consapevole, qualsiasi falsa informazione circa morte, ferite, malattie, sfregi, condotte indecenti, o condotte criminali, della persona destinataria del

[7] Ibidem nota 6
[8] Ibidem nota 6

messaggio o a qualsiasi membro della famiglia del destinatario, con lo scopo di abusare, dare fastidio, minacciare, terrorizzare, molestare o imbarazzare.
- Permettere che qualcuno usi un'apparecchiatura elettronica per gli scopi illegali descritti.

Nel caso del North Carolina si rivelano interessanti differenze. Prima di tutto viene allargata la sfera della protezione dall'atto criminale a tutta la famiglia e a tutte le persone che hanno relazioni significative con il destinatario delle minacce o delle molestie, così come essa viene estesa alle sue proprietà. Viene ribadito che l'azione deve essere ripetuta nel tempo. Viene inoltre contemplata una responsabilità oggettiva, qualora il mezzo elettronico fosse stato incautamente custodito ed usato da terzi per effettuare del Cyberstalking.
Il legislatore del North Carolina si e' anche preoccupato che l'interpretazione della sezione relativa al Cyberstalking non potesse essere interpretata per danneggiare qualche attività protetta dalla Costituzione, come ad esempio libertà di parola, protesta o libertà di assemblea. Viene infatti esclusa dalla sezione qualsiasi atto non violento o pacifista, e qualsiasi attività, non minacciosa, intesa a esprimere opinione politica o a fornire informazioni legali ad altri.

Si deve poi inserire una distinzione che appare fondamentale: nel caso delle minacce, di solito non è la minaccia che crea il danno, ma l'atto che ne segue. Il messaggio inviato dal Cyberstalker può essere invece performativo, creando direttamente un dolo (come ad esempio un mail bombing).

La definizione Cyberstalking si può quindi così sintetizzare:

> *il perseguire un'altra persona e/o i suoi familiari in modo premeditato e ripetuto nel tempo, tramite sistemi di comunicazione elettronica o informatica; inviando parole di minaccia alla persona o alla proprietà, incitando terzi a molestare la persona o la proprietà, utilizzando i mezzi di comunicazione stessi come strumenti di dolo.*

Si possono poi identificare due situazioni di Cyberstalking:
- Le attività di Cyberstalking che avvengono on-line e che rimangono confinate nel Cyberspace
- Le attività di Cyberstalking che iniziano nel Cyberspace e che poi continuano anche nella vita reale

Questa differenza dal punto di vista legislativo non e' banale, in quanto alcuni stati nazionali consentono la persecuzione del Cyberstalking solo nel caso in cui questo sia associato ad eventi reali con minacce fisiche, altri anche nel caso in cui le minacce siano solo fatte all'interno del Cyberspace, altri ancora coprono entrambe le situazioni.

E' anche opportuno chiarire gli elementi più caratterizzanti dell'atto illegale e che sono utilizzati per il riconoscimento pratico dello stesso:

- **Obiettivo della minaccia**. L'obiettivo deve essere una persona fisica o una proprietà. Attacchi diretti ad aziende o gruppi in termini generali o per esempio a canali IRC, non sono considerabili Cyberstalking[9].

- **Premeditazione**. Il senso è che l'attacco deve essere premeditato ed organizzato in precedenza. Nel caso che si perda il controllo in una sporadica situazione, a causa di fatti contingenti, non può essere definito come Cyberstalking[10].

- **Procurata angoscia**. Difficile da definire; in ogni caso una situazione di Cyberstalking può essere considerata tale solo se la vittima, in pieno possesso delle sue facoltà mentali, ha paura, e' angosciata dalle minacce in modo tale da avere effetti nella vita reale. Nella legislazione americana vi e' un preciso riferimento al temine "*reasonable reaction*", intendendo che la persona oggetto di questi attacchi deve reagire in un modo "ragionevole" e non mostrare una reazione esagerata (*over-reaction*). Da un punto di vista legale, sempre negli USA, e' necessario che la procurata angoscia sia provata attraverso un "trusted witness" cioè il parere di un professionista medico esperto, che certifichi lo stato della vittima e che testimoni l'effetto che l'incidente ha avuto su di essa[11].

- **Avvertimento ad interrompere la molestia**. In alcuni casi processuali si e' verificato che il Cyberstalker si sia salvato rispondendo alle accuse con l'affermazione che la vittima lo aveva incitato a continuare (in modo più o meno evidente); in altre parole la vittima non era stata in grado di provare che avesse espressamente invitato il Cyberstalker a terminare le molestie. E' quindi necessario, per poter provare che si sia verificato un atto di Cyberstalking, che sia stato espressamente richiesta l'interruzione della molestia e che l'atto sia comunque continuato anche successivamente alla richiesta[12]. Nel Cyberspace, in mezzo a simulazioni e giochi di ruolo diventa a volte difficile per l'investigatore capire dove comincia e dove finisce un gioco. Per fare un esempio uno studente della Columbia University che aveva fisicamente violentato una compagna di corso fu assolto anche se non c'erano dubbi sulla violenza; l'assoluzione fu un atto obbligato perché il ragazzo portò una serie di messaggi di posta elettronica nei quali la ragazza, probabilmente per uno stupido gioco, diceva di amare il sesso violento[13].

- **Molestia (Harassment)**. La molestia, come già detto, può essere definita come un atto intenzionale, non consentito e ripetuto, che, diretto ad una persona, l'allarma, la terrorizza, la tormenta causandole la sofferenza di angosce emotive a fronte di questi attacchi[14]. Per essere considerato un reato di Cyberstalking, la vittima deve essere nelle sue piene facoltà mentali ed aver mostrato una "*reazione ragionevole*".

---

[9] Si veda http://www.cyberangels.org, http://www.crimelibrary.com/criminology/cyberstalking/, referenze accedute il 30/04/2005
[10] Ibidem nota 9
[11] Ibidem nota 9
[12] Ibidem nota 9
[13] Laura Barandes ,"Focus on New York's Rape Shiled Law", Court TV, 22 Dicembre 1999, ottenibile da HTTP://www.courttv.com/national/1999/1223/jovanovic_ctv.html, pagina acceduta il 22/04/2005. La *Rape Shield Law* e' una legge con lo scopo di proteggere la vittima di un reato a sfondo sessuale dall'essere ingiustamente diffamata basandosi su passati comportamenti della vittima in modo da condizionare l'opinione della giuria.
[14] Lo statuto della California definisce la molestia come "[...]a knowing and willful course of conduct directed at a specific person that seriously alarms, annoys, torments, or terrorizes the person, and that serves no legitimate purpose. This course of conduct must be such as would cause

- **Litigi (Flame War)**. In Internet qualche volta si assiste a quello che viene chiamato "*Flame War*". Durante uno di questi litigi, due o più persone si scambiano parole pesanti su newsgroups, per posta elettronica o altri mezzi comunicativi. Il litigio e' reciproco nel senso che tutti i partecipanti inveiscono gli uni contro gli altri. E' questo l'elemento distintivo rispetto al Cyberstalking. Può succedere però che un litigio si trasformi in Cyberstalking, nel caso in cui uno dei litiganti smetta e l'altro no; anche se invitato a smettere questo continua a mandare insulti per posta o similari. A quel punto si può parlare di Cyberstalking[15]. Gli incontri vis-à-vis sono facilitati in termini di ricerca dell'accordo, mentre quelli mediati da computer generano più facilmente dissenso. Le ricerche svolte hanno appurato che l'impressione on-line che si costruisce dell'interlocutore è la causa più frequente di questi malintesi e dissensi. Si verifica una sorta di reazione a catena. Da una parte quello che si riesce a dire digitando parole su una tastiera è probabilmente diverso da quello che si direbbe di persona, e gli altri reagiscono a questo atteggiamento alterando di conseguenza il loro comportamento. Dall'altra la condizione di anonimato e la protezione, che essa infonde, porta alcuni ad essere meno inclini a seguire le convenzioni del controllo sociale mediato attraverso le microinterazioni interpersonali. Nel momento però in cui questi comportamenti diventano comuni, perdono la loro forte valenza deviante, e di conseguenza criminale.

Definire i confini dell'attività di Cyberstalking non e' semplice ed essi variano a seconda del legislatore. Un buon esempio di questa difficoltà e' cercare di capire dalla letteratura se le implicazioni di pedofilia del Cyberspace debbano essere incluse, ed in che termini, nel Cyberstalking.

Nel caso di un bambino, la protezione legislativa dovrebbe essere più estesa, in quanto la soglia di danneggiabilità dell'emotività del bambino e' sicuramente più bassa di un adulto. Il bambino ha inoltre delle capacità limitate di separazione tra il giusto e lo sbagliato, tra il gioco e la vita reale. L'inviare per esempio messaggi atti ad adescare minori a fini di molestie sessuali potrebbe essere inserito nelle definizioni degli atti illegali legati al Cyberstalking.
Tipicamente vengono perseguite solo le azioni di adescamento fisico. Quelle perpetuate nel Cyberspace possono essere altrettanto pericolose e la loro regolamentazione sarebbe un contributo alla lotta alla pedofilia.
Infatti, questi atteggiamenti, oltre alla minaccia e alla paura immediata della vittima, devono essere presi seriamente in considerazione, perché sono molto spesso preludio di atti di maggiore violenza, sia nei casi con minori che con adulti; in uno dei casi più drammatici di Cyberstalking, un uomo nel New Hampshire, dopo aver ripetutamente minacciato la sua vittima per posta elettronica, l'ha poi effettivamente uccisa[16].

A protezione dei bambini, ed in attesa di una legislazione più puntuale, l'allora Ministro dell'Istruzione americano Richard W. Riley (Segretary Department of Education) ha pubblicato nel 1997 (e poi successivamente aggiornato) un volume di informazione su Internet intitolato

---

a reasonable person to suffer substantial emotional distress, and must actually cause substantial emotional distress to the person". Integrabile con quella del Michigan : "[...]conduct directed toward a victim that includes, but is not limited to, repeated or continuing unconsented contact, that would cause a reasonable individual to suffer emotional distress, and that actually causes the victim to suffer emotional distress". Essa include il concetto di ripetuta azione, di consenso e di "reasonable individual".

[15] Si veda http://www.cyberangels.org, referenza acceduta il 24/04/2005

[16] Il Giorno del 14 Giugno 2000, da http://ilgiorno.monrif.net/art/2000/06/14/1013323.html, pagina acceduta il 22/04/2001

"Parents Guide to the Internet"[17] nel quale vengono forniti consigli utili ai genitori su come controllare l'attività dei figli nel Cyberspace. Sono incluse anche alcune "regole" che dovrebbero essere insegnate ai bambini. Vediamone insieme alcune:

- non dare mai informazioni personali come nome, indirizzo di casa, numero di telefono, età, razza, reddito familiare, nome o indirizzo della scuola, nome o indirizzo di amici
- non condividere mai la userid e password con altri, anche se sono vostri amici
- non incontrare mai una persona che si e' conosciuta nel Cyberspace, a meno che un tuo genitore non sia informato, ti accompagni, e che l'incontro si svolga in un posto pubblico ed affollato
- non rispondere mai a messaggi che sembrano strani, o che lasciano confusi. Ignorare chi lo ha mandato e avvertire immediatamente un tuo genitore
- non usare mai un linguaggio non appropriato in messaggi e non minacciare altre persone anche se per gioco.

A testimonianza dell'importanza del fenomeno, lo stesso Presidente Clinton incluse un "*Message to parents about Internet*" nello stesso volume. Esistono anche centri di supporto[18], a cui i genitori americani possono rivolgersi, che pubblicano manuali educativi e che organizzano eventi informativi. Una delle maggiori pubblicazioni e' "*The parents' Guide to the Information Superhighway: Rules and Tools for Families On-line*"[19] preparato dalla *Children's Partnership Organization.* Lo stesso Federal Bureau of Investigation (FBI) ha distribuito un volume intitolato "*Parent's Guide to Internet Safety*"[20] sullo stesso tema.

Per gli adulti, si sono moltiplicate le organizzazioni a supporto delle vittime del Cyberstallking e per fornire informazione preventiva. Molti di essi danno consigli su come evitare guai in rete, vediamone alcuni:

- Tipicamente il molestatore si eccita con la sua condizione d'anonimato che lo fa sentire molto forte nei confronti della vittima. Ignorare sempre i messaggi e non rispondere. A meno che non s'incontri qualcuno che ha veramente turbe psichiche o persegue depravazioni, quest'atteggiamento porta il molestatore a perdere interesse velocemente.
- Allo stesso modo non rispondere mai a provocazioni on-line (*flaming*)
- Se si e' in ambienti quali MUD o IRC, scegliere un soprannome (*nick-name*) che sia neutro sessualmente.
- Cercate di evitare situazioni di flirt on-line, a meno che non siate fortemente preparati ad affrontarne le conseguenze.
- Salvate sempre tutti i messaggi d'offesa e/o molestia e fateli avere al vostro ISP.
- Se avete la sensazione d'essere oggetto di Cyberstalking avvertite immediatamente la Polizia.
- Non date mai nessuna informazione personale, vostra o dei vostri familiari

---

[17] Il documento può essere ottenuto da http://www.ed.gov (gli editori del sito consigliano di usare il locale motore di ricerca per localizzare il documento, in quanto le pagine cambiano molto spesso)
[18] Alcuni gruppi di supporto sono *Safeguarding Our Children United Mothers* (http://www.soc-um.org), *Safe Kids Home Page* (http://www.safekids.com/), *Kid Safe* (http://www.kidsafe.com), Child Safety on the Information Highway (http://www.4j.lane.edu/safety/childtoc.html)
[19] Il documento può essere ottenuto da http://www.childrenspartnership.org (gli editori del sito consigliano di usare il locale motore di ricerca per localizzare il documento, in quanto le pagine cambiano molto spesso)
[20] Il documento può essere ottenuto da http://www.FBI.gov (gli editori del sito consigliano di usare il locale motore di ricerca per localizzare il documento, in quanto le pagine cambiano molto spesso)

- In caso di problemi con qualcuno scollegatevi immediatamente e non ricollegatevi, se potete, per qualche giorno

In Italia è stato recentemente introdotto un "113" per i reati perpetuati per via informatica; si può accedervi tramite un call center ed il portale della Polizia di Stato: www.poliziadistato.it/pds/informatica/index.htm

Profilo delle vittime

Dal punto di vista della differenziazione di genere, si rivela una forte caratterizzazione. I dati confermano che la maggioranza dei Cyberstalkers sono di sesso maschile e che le vittime sono di sesso femminile, anche se ci sono stati casi di vittime di sesso maschile attaccate da donne, o attacchi tra omosessuali[21].
Cyberangels, l'organizzazione senza fini di lucro che dal 1995 aiuta le vittime del Cyberstalking, indicava che nel 2001 l'83% delle vittime era di sesso femminile[22]. Il fenomeno sembra però essere di avvicinamento tra i due gender; mentre il valore cumulato 2000-2004 risulta essere del 78%, questo scende considerevolmente per il solo 2004, arrivando al 69%[23]:

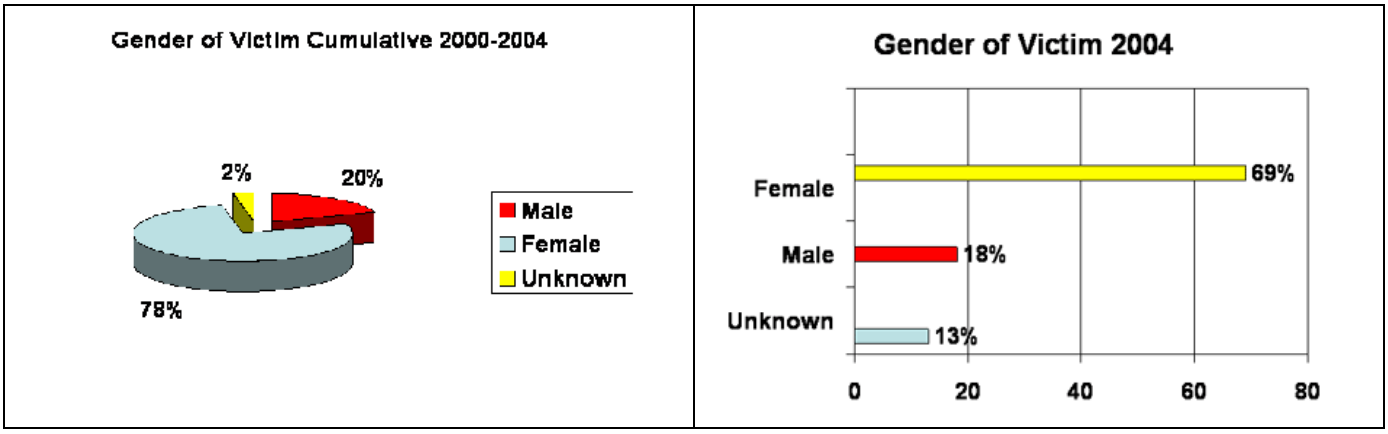


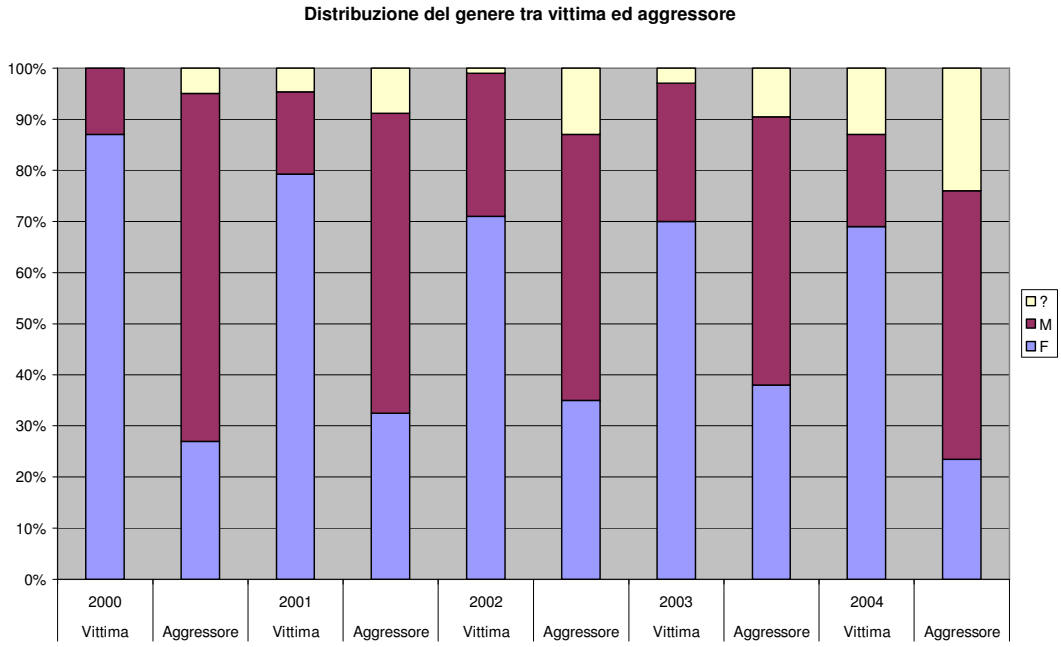
Figura 1 - Distribuzione per genere (fonte WHO@)

Dal momento che la popolazione femminile in Internet e' numericamente di molto inferiore a quella maschile[24], una delle possibili cause del Cyberstalking e' che i frequentatori maschili siano frustrati da non poter avere una risposta adeguata alle loro richieste di compagnia femminile rimanendo urtati nel loro ego maschile che, essendo stato piantato in asso, vuole una rivincita[25].
Le stesse donne che frequentano il Cyberspace sono molte volte curiose, poco pratiche, e si lasciano coinvolgere in attività che considerano un gioco, e per le quali non seguono le normali

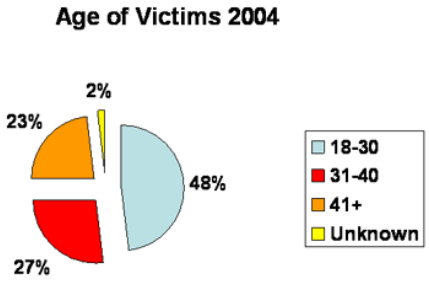
[21] CyberGuards, da http://www.cyberguards.org/CyberStalking.html, pagina acceduta il 22/04/2005
[22] Si veda http://www.cyberangels.org/stalking/victim.html, acceduta il 24/04/2001
[23] Fonte WHO@, http://www.haltabuse.org/resources/stats/genderv.shtml, acceduta il 30/04/2005
[24] Non sono disponibili stime precise. E' praticamente impossibile censire l'intera popolazione di Internet, ma la percezione degli operatori (non scientificamente provata) e' che il numero degli uomini su internet sia in rapporto di 3 a 1 rispetto alle donne. Altri (http://www.cyberangels.org/stalking/sharassment.html) dicono 2 a 1. In ogni caso la competizione per l'attenzione femminile e' molto forte.
[25] Ibidem nota 22

prudenze e scetticità a cui le donne sono abituate ad affidare la propria incolumità nel mondo reale[26].

E' anche interessante notare come al pari di una diminuzione delle frequenze del genere femminile tra le vittime, ci sia un incremento dello stesso genere per il genere dell'aggressore[27]:

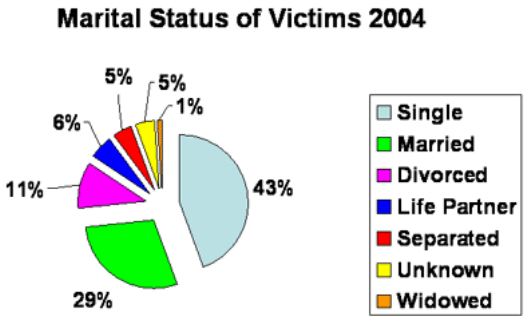


Da un punto di vista dell'età viene riportata una forte concentrazione sotto i trent'anni (48%) e comunque il 75% delle vittime ha meno di 40 anni[28] con un trend abbastanza stabile dal 2000 ad oggi.



Lo stato coniugale vede una prevalenza dei single per il 43% seguito da un 29% di persone coniugate; anche questa distribuzione appare abbastanza stabile nel periodo 2000-2004:

[26] Anche in molti reati di violenza fisica specifici (come lo stupro, o le molestie sessuali etc), la maggior parte delle vittime sono di sesso femminile. Questo può essere generalmente spiegato da un punto di vista sociologico grazie ad un'asimmetria strutturale nella divisione sociale del potere tra i generi che porta gli uomini ad aver più potere delle donne. In rete questo fenomeno è accentuato per un fenomeno di maggioranza-minoranza e per un fattore di potere tecnico (gli uomini sembrano essere più competenti in linea di massima)
[27] Fonte elaborazione su dati inviati via email su richiesta dell'autore all'organizzazione "Work to Halt Online Abuse" (maggio 2005).
[28] Fonte indagine 2004 "Work to Halt Online Abuse".



Un elemento è comune a tutti i casi esaminati ed attinenti all'argomento: il Cyberstalker e' un cacciatore di debolezza, sia questa una debolezza di conoscenza in merito ad Internet, sia questa una debolezza emotiva, sia questa una debolezza fisiologica (minori o persone con handicap). Il Cyberstalker cerca la possibilità di aver un controllo ed un rapporto *master-slave* con la vittima.

E' per questo che l'apparire insicuro in rete, usare soprannomi sbagliati, fare domande o dare risposte che rivelino l'identità di genere piuttosto che la propria inesperienza con il mezzo utilizzato, richiama l'attenzione del Cyberstalker; molte vittime sono nuovi utenti della rete che non hanno ancora familiarizzato con i suoi pericoli[29].
Allo stesso modo le persone che si rivolgono ad Internet per avere un'avventura romantica o per cercare rimedi alla solitudine sono le vittime preferite di questo genere di atti criminali. Spessissimo la vittima ed il persecutore avevano una precedente relazione e gli attacchi sono cominciati nel momento in cui uno dei due ha tentato di troncare la relazione.

Ci sono stati, ad ogni modo, casi tra perfetti sconosciuti. Vista la facilità di reperire informazioni su Internet, non e' difficile procurarsi informazioni anche su perfetti sconosciuti che diventano ottime vittime potenziali[30] , ed anzi, in alcuni casi e' proprio questo che si e' rilevato essere l'elemento che dà soddisfazione al persecutore.

L'aspetto di debolezza nel Cyberspace viene poi portato anche nella vita reale, quando le vittime pensano che l'attacco sia stato causato da qualche loro azione incauta; rientra infatti nel profilo classico di vittima un senso di impotenza e di giusta punizione per aver commesso l'imprudenza stessa[31]. Una volta sotto minaccia, invece di pensare alle possibili reazioni e a come denunciare il molestatore, esse si avvitano in un rapporto di attrazione /repulsione con la situazione, dimenticando che in molti dei casi sarebbe possibile risolvere il problema scrivendo un messaggio all'Internet Service Provider, cambiando identità di rete, o scollegandosi dalla stessa per un po' di tempo.

[29] "CyberAngels.org, the largest Internet Safety Organization since 1995", http://www.cyberangels.org/stalking/index.html, Online guide.
[30] Si veda il paragrafo "Come le nuove tecnologie aggravano il problema" a pag. 15
[31] Ibidem nota 22

Profilo del Cyberstalker medio

Come si e' visto il Cyberstalker e' tipicamente di sesso maschile, può conoscere la vittima fisicamente o può non averla mai incontrata, può vivere accanto alla vittima o essere in un'altra nazione a migliaia di chilometri di distanza.
E' comunque un individuo che si deve sentire in controllo sulla vittima. Ricava da questo controllo la sua eccitazione e la spinta a continuare nella molestia. E' per questo che nei casi in cui il molestatore non conosce la sua vittima, egli può provare la stessa eccitazione nell'attività di ricerca d'informazione sulle possibili vittime, utilizzando a volte tecniche informatiche molto sofisticate e complesse.
La pulsione di giocare con la vittima come un gatto con un topo, assaporando l'impossibilità della vittima di sfuggire, è l'elemento che probabilmente alimenta il Cyberstalker. L'esercizio del suo controllo, passa da una dimostrazione di forza al perdurare della stessa, trasformandola in potere. Il Canetti considera la forza più immediata del potere[32] e quando la forza perdura essa diviene potere, per ritrasformarsi in forza nel momento culminante del potere stesso. E come nel gioco del gatto con il topo, la vittima una volta catturata è in balia del Cyberstalker. Il gatto ha afferrato e ucciderà il topo, ma quando il gatto lo lascia andare, in quel momento esso non è in balia del suo persecutore; il gatto ha però pienamente il potere di riprendere il topo. Lo ha lasciato andare, ma lo lascia fuggire solo nell'ambito del raggio d'azione della sua forza e, finchè il topo rimane in essa, è in suo potere. Quello che il Canetti chiama potere si può identificare negli attimi di terrore del topo e nello spazio sul quale il gatto proietta la sua influenza. Similmente il Cyberstalker utilizza il mezzo telematico come prova di forza ed il Cyberspace stesso come spazio, riuscendo a volte ad espandere il raggio di azione anche nella vita reale, con sgomento e sconforto delle sue vittime.

Quello che fa la differenza e che consente di effettuare una minima tipizzazione del Cyberstalker sta nelle motivazioni che lo hanno portato a scegliere la sua vittima, motivazioni che ne modelleranno il comportamento nell'azione delittuosa. Tre tipi di Cyberstalker sembrano includere la maggioranza dei casi denunciati:

- ossessivo
- sognatore
- vendicativo

Il Cyberstalker ossessivo e' qualcuno che non vuole credere che un rapporto od una situazione sia finita nonostante l'altro partner gli abbia detto in vario modo che non ci sono i presupposti per continuare. Durante la loro relazione questi individui sono spesso possessivi e talvolta hanno precedenti penali per reati diversi da quelli del Cyberstalking. E' la tipologia più diffusa[33].

Il Cyberstalker sognatore non ha avuto tipicamente nessun contatto reale con la vittima, ma nel loro immaginario. Possono soffrire di malattie psichiche tipo schizofrenia, sdoppiamento della personalità ed erotomania. Si relazionano con la vittima costruendo un falso rapporto basato unicamente sulla loro immaginazione. Nel caso degli erotomani essi credono che la vittima sia innamorata di loro, anche se probabilmente non si sono mai incontrati.

---

[32] Elias Canetti, "Massa e potere", Biblioteca Adelfi, 1997, pagina 339
[33] Si veda http://www.cyberangels.org/stalking/stalker.html, acceduta il 24/04/2001

Un'altra situazione può essere quella dove il predatore pensa che il destino lo abbia scelto per vivere vicino alla vittima (anche se mai incontrata). L'atto criminale diventa così un modo per dimostrare il suo amore e conquistare l'attenzione da parte della persona amata. In questo caso la vittima può essere un terzo individuo ignaro della persecuzione. Un buon esempio di questo tipo di stalking (non cyber in questo caso) e' quello di John Hinckley Jr. che sparò al presidente Reagan per dimostrare il suo amore a Jody Foster[34].
Questo tipo di aggressore è solitamente solitario, scapolo, ha difficoltà a relazionarsi socialmente, a mantenere una relazione di amicizia o sentimentale. Spesso ha difficoltà negli incontri sessuali (rari o addirittura assenti del tutto). Le vittime sono quasi sempre partner impossibili; celebrità o professionisti che hanno frequentato, come dentisti, dottori, avvocati, insegnanti. Sono spesso difficili da identificare, e la persecuzione può andare avanti per molto tempo.

Il Cyberstalker vendicativo sceglie la sua vittima perché si sente da essa offeso. L'offesa può essere reale o immaginaria. Cercano in pratica di pareggiare un conto aperto e per questo si sentono vittime più che predatori. Molti casi si trovano in situazioni di impiegati che sono scontenti del modo con cui un capo o l'azienda li ha trattati, altri hanno contemplato ex-coniugi. In ogni caso questo Cyberstalk e' pericoloso perché l'epilogo e' quasi sempre un epilogo di violenza fisica.

Nel caso di attacchi a minori, il predatore e' quasi sempre un adulto.

I Cyberstalker non seguono l'idelatipo del criminale: sono solitamente non violenti, hanno una buona posizione sociale e/o cultura medio-alta, hanno buone capacità di programmazione comportamentale, tendono alla solitudine e non si percepiscono come dei criminali. Minimizzano, inoltre, il rischio di essere individuati e catturati e si comportano frequentemente come attivati da una percezione ludica delle loro incursioni, come se la loro azione fosse ambientata in un video gioco[35].
"Potrebbe essere il bravo ragazzo della porta accanto, lo studente modello, il dipendente timido: tutte tipologie di persone che non sarebbero mai in grado di fare del male se avessero la loro vittima davanti: vengono meno i freni inibitori, in quanto tra il soggetto agente e la vittima si interpone in computer, attuandosi, in tal caso, la c.d. "spersonalizzazione" nel reato"[36].

In alcuni soggetti si rileva una difficoltà ad identificare il limite che separa la realtà dal virtuale o nel potersi spostare dinamicamente e velocemente dal virtuale al reale (anche dopo una lunga permanenza nel virtuale) mantenendo una lucida percezione e controllo dei propri comportamenti, valutazioni e significazione delle azioni[37].

Differenze tra molestie off-line e quelle on-line

Il fatto che il Cyberstalking non coinvolga un contatto fisico può creare l'impressione che questo fenomeno sia meno allarmante di quello off-line. L'impressione e' sicuramente falsa e

[34] Ibidem nota 33
[35] Ibidem nota 1, paragrafo: "influenza digitale sul crimine"
[36] Monica delle Donne, "Tecniche di indagine nell'ambito dei reati informatici", 2004, Diritto&Diritti
[37] Ibidem nota 1

probabilmente e' stata la causa del ritardo con cui la società ha iniziato a costruire una risposta legislativa al fenomeno.
Proviamo ad analizzare più a fondo le differenze tra uno *Stalking* ed un *Cyberstalking*.

Similitudini

In entrambe le situazioni, la maggioranza dei casi coinvolge persone che si trovano in relazione d'intimità, amicizia o parentela. Casi che coinvolgono sconosciuti avvengono, ma sono molto più rari

In entrambe le situazioni, la maggioranza delle vittime sono donne. La maggioranza dei molestatori sono uomini.

In entrambe le situazioni, chi molesta è eccitato dal controllo sulla vittima.

Differenze

Lo *Stalking* di tipo off-line richiede che sia chi compie l'atto criminale che la vittima risiedano nella stessa area geografica. Nel caso on-line, ovviamente, i due possono essere anche a migliaia di chilometri di distanza.

Le comunicazioni elettroniche amplificano il problema nel caso dell'on-line, dando la possibilità di effettuare delle operazioni in modo automatico e consentendo di impersonificare altre persone (si veda il prossimo paragrafo).

Nel caso dello Stalking, il molestatore deve avere il coraggio di affrontare la vittima in modo fisico (anche se solo con la voce attraverso il telefono). Questo confronto a volte e' un inibitore che blocca l'azione criminale, ma che viene completamente rimosso nel caso del Cyberstalking, in quanto il contatto fisico non esiste.

Il celare la propria identità e l'agire sotto anonimato è molto più semplice nel caso del Cyberstalker.

Il periodo di azione è tipicamente più breve nel Cyberstalking. Anche se il periodo varia a seconda del tipo di crimine, nel caso off-line si ha una media di 1,5 anni con punte fino ai 10 anni per gli erotomani. Nel caso dei Cyberstalker il periodo più corto è di 2 settimane fino ad un massimo di 38 mesi. Un'ipotesi alla base di questa differenza risiede sulla maggiore efficienza che ha il mezzo informatico (come nel mondo professionale) per cui si può compiere l'azione più velocemente (ad esempio ricercare dati sulla vittima o tracciarne le attività[38].

Diverso è anche il concetto di corpo del reato e di cose pertinenti al reato.
In Italia, infatti, il comma 2 dell'art. 253 codice di rito, "indica quale corpo del reato non solo le cose sulle quali o mediante le quali il reato è stato commesso, ma anche quelle che ne costituiscono il prodotto, il profitto o il prezzo, comportando, quindi, la non conciliabilità della definizione materiale data dal legislatore con la natura immateriale delle tracce informatiche, di guisa che non se ne può prospettare il furto ma solo la duplicazione abusiva"[39].

---

[38] Si veda Paul Bocij, Mike Sutton, "Victims of Cyberstalking: Piloting a Web-Based Survey Method and Examining Tentative Findings", 2004, ottenibile da http://josi.spaceless.com/article.php?story=20040214050558297, copia del 10-05-2005
[39] Si veda [Delle Donne 2004]

> La giurisprudenza non ha saputo dare risposte esaurienti riconoscendo sia la natura del computer di corpo di reato, sia di mezzo attraverso il quale si è perpetrato il reato, sia di elemento pertinente al reato, il cui esame potrebbe dimostrare il fatto criminoso nel suo complesso.

Emile Durkheim affermava che un atto non urta la coscienza perché è criminale, ma che è criminale in quanto urta la coscienza comune. Le risposte della collettività variano considerevolmente secondo il luogo, per cui un atto può essere considerato deviante solo nel contesto socioculturale in cui ha luogo. Nel caso del Cyberstalking, gli atti possono avvenire in un contesto socioculturale transnazionale, aprendo vari interrogativi sul significato di devianza dell'atto stesso ed introducendo non pochi problemi di competenza giurisdizionale.

La possibilità poi di celare la propria identità è sicuramente un fattore che allenta il controllo sociale su questi individui e facilita lo scivolamento verso un comportamento deviante. Questi individui vedono nel ruolo del Cyberstalker, e nel potere che esso gli regala, un momento di riscatto e di fuga dalle tensioni che alcune società occidentali come quella americana introducono con la loro differenza tra le mete di successo economico professate e l'effettiva distribuzione dei mezzi necessari al loro raggiungimento.

C'è poi l'aspetto della mancanza di regole in alcuni ambienti del Cyberspace che potrebbe, per dirla alla Emile Durkheim, portare ad un comportamento anomico non essendo chiaro per un navigatore del Cyberspace cosa è giusto e cosa non lo è, oppure cosa si possa considerare gioco e cosa no.

Come le nuove tecnologie aggravano il problema

Una della grandi differenze tra lo stalking reale e quello nel Cyberspace e' la facilità con la quale il molestatore può automatizzare azioni che producano molestie o minacce.
Per un Cyberstalker non e' difficile mandare messaggi ad orari casuali e/o improbabili, mentre lui non e' fisicamente davanti al suo PC e mentre magari sta vivendo la parte "normale" della sua esistenza lavorando di fronte al pubblico in un qualunque ufficio.

Inoltre, Internet consente a persone esperte di prendere il controllo di strumenti che sono al di fuori del Cyberspace come ad esempio il telefono, il fax, il conto in banca, la luce, il gas eccetera eccetera.

Un fenomeno simile sta accadendo in Italia ma attraverso una tecnologia che qui è molto più diffusa di Internet: i telefoni cellulari. Il messaggio SMS e' stato usato come veicolo tecnologico da alcuni Cyberstalkers. Nel febbraio 2001, un articolo del quotidiano "il Giorno"[40] denunciava una forte attività di molestia a sfondo sessuale in Toscana, apparentemente iniziata nel dicembre del 2000. La Polizia Postale, l'organo di controllo che in Italia ha la competenza per i reati commessi attraverso mezzi di comunicazione, continua oggi a ricevere numerose segnalazioni di molestie perpetuate attraverso canali di comunicazione elettronica.

---

[40] Il giorno, edizione del 14 Febbraio 2001,"Molestie via Telefonino, nuovo campo di indagine della Polposta", ottenibile da http://ilgiorno.monrif.net/art/2001/02/1471824505, copia del 20/04/2001.

Nel caso del telefonino, gli investigatori hanno la possibilità di chiedere agli operatori telefonici i così detti "*Call Data Record (CDR)*" che consentono l'individuazione di chi ha inviato il messaggio. E' proprio Internet però a complicare la situazione, dal momento che da qualche tempo e' possibile inviare messaggi SMS tramite portali WEB. In questo caso, il numero originario del messaggio SMS risulterà essere quello dell' Internet Service Provider, e non sarà possibile facilmente arrivare a chi ha lanciato il messaggio.

Sarebbe quindi auspicabile una regolamentazione simile a quella in essere per gli operatori telefonici che consenta di effettuare un tracciamento a ritroso del messaggio di molestia. Lo stesso articolo afferma che, dal Settembre 2000, 15 autori [41]di queste molestie sono stati identificati e denunciati alla magistratura; quindi anche in assenza di regolamentazione, anche se non in tutti i casi, e' possibile risalire all'autore del reato e sanzionarlo.

In California alcuni Cyberstalker hanno compiuto molestie simili inviando messaggi su Pagers (i nostri vecchi *teledrin*) contenenti il numero 187 che corrisponde al codice della sezione penale che descrive l'omicidio.

La tecnologia consente, inoltre, ad un esperto di impersonare un altro utente. In questo modo il molestatore può restare nell'ombra inviando messaggi per nome e per conto della vittima che ne pagherà le conseguenze. Esempi di questa tecnica sono ordinare merce utilizzando le carte di credito della vittima e mandandogli a casa centinaia di oggetti inutili, richiedere servizi telefonici o televisivi (cable TV) per conto della vittima, o suscitare sdegno insultando gente nel Cyberspace utilizzando l'identità della vittima.
Le reazioni a queste molestie sono terribili e la vittima si sente impotente perché non sa chi colpire. Anche le istituzioni di tutela sono disarmate, perché a tutti i controlli risulterà sempre che era stata la vittima ad effettuare quelle operazioni.

Internet e' il regno del Cyberstalker ed essa viene utilizzata per ottenere tutte le informazioni che occorrono per creare il danno e per poi perpetuare il reato stesso. Ma come fa il Cyberstalker a procurarsi queste informazioni, alcune delle quali veramente private negli Stati Uniti, come il Social Security Number[42].? Vediamo di spiegarlo raccontando una lotta legale tra la Banyan Systems ed il proprietario di un sito, diciamo non proprio ortodosso, Glen Roberts[43].

Banyan, un'azienda multinazionale leader nel settore delle telecomunicazioni, si era infuriata perchè il sito di Roberts, the Stalker's Home Page, conteneva un riferimento ad un sistema di pagine bianche chiamato Switchboard che era gestito da una società posseduta dalla Banyan[44].
Il caso e' interessante perché il sito di Roberts aveva lo scopo di denunciare la disponibilità di informazioni private sulla rete e di come questo violasse la privacy delle persone; in pratica era (o meglio è) un super indice di tutte le banche dati liberamente accessibili e che contengono ogni tipo di informazioni.

---

[41] La tipologia di questi responsabili e' varia; ad esempio donne e uomini lasciati dai rispettivi partner, rivali in amore, e studenti in vena di scherzi pesanti.
[42] Il Social Security Number è l'analogo del nostro Codice Fiscale. Negli Stati Uniti non è pubblico e viene utilizzato per verificare l'identità delle persone quando vengono effettuate delle operazioni amministrative per telefono o per via telematica.
[43] Jim Davis, CNET News, "Stalker's home page scares Banyan", June 1996, ottenibile da http://news.com.com/2100-1023-215869.html?legacy=cnet, acceduta il 2/05/2005.
[44] La società posseduta da Banyan e' la Coordinate.com

Nel caso dello switchboard Roberts aveva dimostrato come usare questo elenco per incrociarlo con un atlante metropolitano e determinare l'esatta abitazione di una persona a partire dal suo numero di telefono, e, partendo dall'abitazione, sapere il numero di telefono. Gli avvocati della Banyan chiesero all'ISP che ospitava il sito di provvedere ad oscurare il sito come dicevano essere richiesto dalla normativa vigente, ma l'ISP non si mosse; l'azione di Roberts fu infatti considerata perfettamente legale: non aveva utilizzato il logo della società, non ne aveva parlato male, ma aveva solamente definito un aggancio al loro sito come parte di un commento perfettamente lecito e sotto la protezione della libertà di espressione.
Inoltre, secondo il parere di David Post, direttore del Cyberspace Law Institute del Georgetown University Law Center, questo aggancio e' una particolare forma di espressione chiamata "hypertext linking" che e' protetta dal Copyright Act[45] ed e' null'altro che il referenziare una fonte di informazioni senza comprometterne i diritti di autore. Forti di questo precedente sono nati molti siti, con obiettivi molto meno nobili di quelli che Roberts aveva all'inizio (o che almeno dichiarava di avere) ed e' oggi relativamente facile trovare siti che forniscano chiare informazioni su come estrarre dati privati ed infrangere anche le più elementari norme sulla privacy.

Per esempio se si accede al sito di Roberts[46], si possono trovare informazioni quali:

- Social Security Number[47] delle 400 persone più ricche in america e dei personaggi pubblici più in vista.
- Video in tempo reale prodotti da telecamere di sorveglianza sulle strade e sui luoghi pubblici
- Pagine bianche degli USA e CANADA
- Elenchi con indirizzi stradali
- Elenchi con tipi di business, elenco degli impiegati, elenchi telefonici aziendali, elenchi con e-mail
- Profili di terroristi, profili stilati dall'FBI, elenchi dei contributi a tutte le campagne elettorali americane
- Mappe di tutte le strade delle città americane
- Prenotazioni di viaggio (aerei, albergo, automobili)
- Registri di proprietà (Immobili, auto, barche)

Il vero problema e' che la disponibilità libera di queste informazioni nella rete infrangono l'unica concreata protezione alla privacy che si e' avuta finora: la frammentazione dei dati e la loro dispersione spaziale e temporale. Nel passato, infatti, questi registri esistevano, ma le informazioni che essi contenevano erano disconnesse e non agganciabili l'una con l'altra. Esse erano disperse sia in termini di depositi che di aggiornamento temporale. La possibilità di navigare liberamente attraverso di loro, deducendo informazioni private prima impossibili da ottenere, crea una grave forma di attentato alla nostra privacy, un attentato che andrebbe regolato da apposite e specifiche leggi. Sarebbe un interessante soggetto di ricerca confrontare queste esigenze con la legge sulla privacy 675/96 o la nuova *196/2003* che è in vigore in Italia.

---

[45] Ibidem nota 43
[46] Si veda http://www.glr.com/stalk.html, copia accesso del 2-5-2005,
[47] Il Social Security Number e' un analogo del codice fiscale in Italia. Il numero non e' pubblico e viene normalmente utilizzato per verificare l'identità delle persone durante transazioni telefoniche e/o on-line.

Il Cyberstalker, sia che conosca la sua vittima sia che non la conosca, utilizza questa disponibilità di informazioni a fini persecutori, riuscendo con un minimo di abilità ad appropriarsi di informazioni che consentono di agire su conti correnti, utenze elettriche e telefoniche, inviare e ricevere telegrammi, acquistare merce tramite carta di credito eccetera. In pratica viene dato modo al Cyberstalker anche di selezionare la vittima in base ad una serie di parametri che gli consentono una probabilità di successo più elevata, come ad esempio il sesso, l'età, la località di residenza, il tipo di lavoro, se si è sottoposta a cure mediche, eccetera.

I numeri del Cyberstalking

Non sono disponibili al momento statistiche ufficiali del fenomeno in Italia. Esistono tuttavia alcune statistiche ufficiali negli USA che possono essere utili per inquadrare i tratti più caratteristici del fenomeno. Ci sono anche statistiche compilate dai maggiori ISP sul numero dei reclami che essi ricevono per situazioni di Cyberstalking che colpiscono i loro abbonati e poche e frammentate informazioni dalle forze istituzionali di controllo.

Per quanto riguarda questo lavoro, dove non espressamente indicato, le informazioni sono state estratte dal rapporto dell'ex Ministro della Giustizia USA Janet Reno[48], che sembra essere al momento la fonte ufficiale più completa ed omogenea[49], anche se ovviamente valida solo per gli USA.

Può essere utile cominciare da alcuni dati che danno uno spaccato del fenomeno delle molestie off-line; secondo un rapporto del National Violence Against Women[50] l'8.3% (8.2 Milioni) delle donne Americane e il 2.2% (2 Milioni) degli uomini hanno subito molestie nelle loro vita. Come visto in precedenza c'è una forte caratterizzazione di genere sia sulle vittime (4 su 5 sono donne) che sui molestatori (87% sono uomini).

Anche la tipologia della relazione con il molestatore ha una caratterizzazione di genere: c'e' un rapporto 2:1 tra donne e uomini nel caso di molestie tra persone sconosciute ed un rapporto 8:1 tra donne e uomini nel caso di molestie tra persone che si conoscevano e si frequentavano. E' molto comune il caso in cui il molestatore sia un coniuge (ex o attuale), un convivente, o una persona con cui si siano avuti appuntamenti intimi (circa 500.000 donne e 185.000 uomini)[51].

Non ci sono dati affidabili sul comportamento del Cyberstalker, ma abbiamo quelli forniti dall' OVC per lo stalking off-line; in un survey compiuto su un campione di studenti americani il 42% degli stalkers avevano seguito la loro vittima, 52% aspettavano dentro o fuori luoghi frequentati dalle vittime, 44% osservavano da lontano, 78% annoiavano via telefono, 31% utilizzavano posta e 25% inviavano posta elettronica[52].

---

[48] 1999 Report on Cyberstalking: a New Challenge for Law Enforcement and Industry; A Report from the Attorney General to the Vice President, disponibile su http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm, pagina acceduta il 24/04/2001, Pagina 5.
[49] Statistiche che non provengono dal rapporto di cui alla nota 48, saranno dichiarate esplicitamente.
[50] "Stalking in America", risultati sull'indagine effettuata dal National Violence Against Women, US Department of Justice, Office of Justice Programs, and Departments of Health and Human Services, Center of Desease and prevention, April 1998, ottenibile da http://www.ojp.usdoj.gov
[51] "OVC Resource Center and the National Criminal Justice Reference Service (NCJRS) 2001 report" ottenibile dal sito del Ministero della Giustizia Americano, http://www.usdoj.gov
[52] ibidem nota 51

Dal punto di vista dei danni procurati alle vittime che non avevano riportato molestie fisiche, un terzo di esse sono dovute ricorrere a cure psicologiche mentre il 7% di esse ha perso il lavoro[53].

Nel 1998 il numero degli utenti Internet Worlwide era cresciuto da 61 Milioni a 147 Milioni in 24 mesi; nel 1999 si arrivò a 320 Milioni. Nel 2005 il totale è di quasi 900 Milioni con un incremento dal 2000 di quasi il 150%; più in dettaglio, la situazione è la seguente[54]:

WORLD INTERNET USAGE AND POPULATION STATISTICS						
World Regions	Population (2005 Est.)	Population % of World	Internet Usage, Latest Data	Usage Growth 2000-2005	Penetration (% Population)	World Users %
Africa	900,465,411	14.0 %	**13,468,600**	198.3 %	1.5 %	1.5 %
Asia	3,612,363,165	56.3 %	**302,257,003**	164.4 %	8.4 %	34.0 %
Europe	730,991,138	11.4 %	**259,653,144**	151.9 %	35.5 %	29.2 %
Middle East	259,499,772	4.0 %	**19,370,700**	266.5 %	7.5 %	2.2 %
North America	328,387,059	5.1 %	**221,437,647**	104.9 %	67.4 %	24.9 %
Latin America/Caribbean	546,917,192	8.5 %	**56,224,957**	211.2 %	10.3 %	6.3 %
Oceania / Australia	33,443,448	0.5 %	**16,269,080**	113.5 %	48.6 %	1.8 %
WORLD TOTAL	**6,412,067,185**	**100.0 %**	**888,681,131**	**146.2 %**	**13.9 %**	**100.0 %**

La crescita dei nuovi utenti può essere stimata in circa 800.000 nuovi utenti per ogni giorno[55].

Non sorprende quindi che, mentre nel 1993 i casi di Cyberstalking furono 640 negli USA, ci si aspetta un numero superiore ai 400.000 per quest'anno. Questi dati sono sicuramente sottostimati perché solo pochi casi vengono censiti e molti di essi rimangono nascosti per anni. Ciononostante tutte le agenzie americane di controllo riportano una preoccupante crescita del fenomeno. Tanto per dare un'idea della sottostima, l'OVC afferma che solo la metà delle vittime femminili di Cyberstalking ad opera di persone a loro vicine ha denunciato il molestatore[56].

Da un punto di vista non governativo, sono disponibili i dati del "Working to Halt On-line Abuse" che dal 2000 ha raccolto informazioni demografiche sulle persone che si rivolgono all'organizzazione per aiuto. Al di là delle informazioni già riportate nel paragrafo "Profilo del Cyberstalker medio", rimane confermato che l'Email è lo strumento usato più spesso e che la California è lo Stato americano con la frequenza di casi più elevati nel periodo (poco meno di 150 casi riconosciuti).

Preoccupante l'incidenza del fenomeno sui minori. L'organizzazione non governativa CyberAngels ha reso noto[57] che su 17 minori collegati su Internet, almeno 1 è stato minacciato o molestato; il 75% dei minori condividono informazioni personali (nome e cognome, età, indirizzo, telefono) in modo consapevole, nella speranza di ricevere in cambio doni. Ben 1 minore su 5 che si collega regolarmente ha ricevuto un qualche approccio sessuale esplicito e 1

---

[53] ibidem nota 51
[54] Fonte "Internet world stats" ottenibile da http://www.internetworldstats.com/stats.htm; copia acceduta il 30/04/2005.
[55] InterGov Office of Public Information
[56] "OVC Resource Center and the National Criminal Justice Reference Service (NCJRS) 2001 report" ottenibile dal sito del Ministero della Giustizia Americano, http://www.usdoj.gov/
[57] Si veda http://www.cyberangels.org/statistics.html, pagina acceduta il 30/04/2005

su 33 seriamente aggredito a scopi sessuali. Il 77% dei giovani americani sono avvicinati prima dei 14 anni, mentre il 22% tra i 10 ed i 13 anni. Questi dati, se pur non ufficiali, confermano la difficoltà di isolare il fenomeno Cyberstalking da quello della Pedofilia on-line, condividendo comunque il problema della scarsità di conoscenza della vera entità dei crimini perpetuati; solo il 25% dei minori dice ai genitori di incontri o proposte di questo tipo e di questi solo il 10% alla fine effettua una denuncia alle autorità competenti[58].

In Italia, da una recente indagine parte del progetto "Pollicino nella Rete" sono emersi dati allarmanti. Il 13% dei minori intervistati ha riferito di discorsi con risvolti sessuali on line, di cui non avevano avvertito i propri genitori o perché se ne vergognavano o perché credevano che loro non li avrebbero capiti[59].

L'ufficio del procuratore del Distretto di Los Angeles ha stimato che il 20% dei casi di molestie gestite dal suo ufficio fossero di tipo elettronico, e stessa percentuale e' stata dichiarata dall'ufficio che si occupa di crimini sessuali nel distretto di Manhattam (NY). Il dipartimento "*Computer Investigations and Technology Unit"* della polizia di New York City ha dichiarato che il 40% dei casi e' collegato al Cyberstalking e che essi sono tutti avvenuti negli ultimi 3 anni. Anche gli Internet Service Provider hanno registrato un forte incremento delle denunce.

Un fenomeno quindi in forte espansione negli USA. Visto il ritardo con il quale l'Europa si muove sul panorama Internet (3-5 anni) e la diversa penetrazione (67% vs 35%) ci sono pochi anni a disposizione per costruire una risposta legislativa specifica ed adeguata a questo problema nel continente Europeo; al momento, come si vedrà, solo l'Inghilterra ha predisposto una protezione giuridica sul tema.

La risposta al Cyberstalking

Riguardo la protezione dei minori dai rischi degli attacchi nel Cyberspace, le istituzioni federali e quelle degli stati locali sono state molto attive sia nella prevenzione che nell'applicazione delle leggi esistenti.
Per esempio, nel 1995, l'FBI lanciò un'iniziativa segreta soprannominata *Innocent Images* per combattere lo sfruttamento minorile attraverso la rete Internet. L'iniziativa non si limitò alla definizione di programmi di indagine, ma portò alla creazione di un centro specializzato di *intelligence*, con sede nel Maryland; il centro e le investigazioni consentirono di perseguire molti molestatori e sfruttatori per un totale di 232 condanne a fine 1998.[60]

A parte l'FBI anche le autorità doganali si interessano al fenomeno e hanno fornito un aiuto nella sua lotta. E' stata creata una specifica sezione chiamata ***CyberSmuggling*** (contrabbando virtuale) per il controllo del contrabbando materiale ed informazioni pornografiche. La sezione fornisce supporto, anche grazie ad un centro di informazioni situato in Virginia, per tutte le

[58] Ibidem nota 57
[59] Monica delle Donne, "Tecniche di indagine nell'ambito dei reati informatici", 2004, Diritto&Diritti
[60] 1999 Report on Cyberstalking: a New Challenge for Law Enforcement and Industry; A Report from the Attorney General to the Vice President, a pagina 2, disponibile su http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm, pagina acceduta il 24/04/2005.

attività che prevaricano i confini degli Stati Uniti[61]; infatti moltissima attività criminale viene svolta nei paesi asiatici e in quelli dell'Europa dell'Est.

Sono stati poi regolamentati sotto una legge federale (la U.S.C. 13032) gli obblighi che i privati hanno, incluso ovviamente gli Internet Service Provider (ISP), in breve:

- di definire regole chiare, all'interno dell'ambiente di rete da loro gestito, per condannare e per combattere qualsiasi attività on-line volta a molestare minori e
- di prendere appropriate azioni qualora un incidente venisse da loro o da altri scoperto.

Sarebbe comunque auspicabile in futuro un ulteriore passo in avanti regolamentando la disponibilità da parte dei genitori di strumenti di controllo quali ad esempio filtri, contatori di tempo, e tracciatura delle attività on-line.

Nell'approccio americano nel combattere il fenomeno si vedono due punti principali:

- la necessità di una professionalità nuova all'interno delle forze di controllo e della magistratura che siano in grado di capire e di combattere il fenomeno, aiutando il legislatore a definire nuove leggi più specifiche, e limitando, cosi, il ricorso a leggi promulgate per combattere crimini simili ma non specificamente di tipo on-line.
- L'importanza della creazione di poli tecnologici a supporto delle iniziative di investigazione, il cui supporto economico deve essere di tipo governativo[62].

Ci sono anche organizzazioni private senza scopo di lucro che costantemente supportano ed aiutano persone con problemi di questo tipo. La più grande e' Cyberangels[63], organizzazione che opera dal 1995 e che riceve circa 300 reclami di Cyberstalking ogni giorno[64]. Un'altra è WHOA che è stata fondata nel 1997 per combattere *l'on-line harassment* attraverso la diffusione pubblica di informazioni e la formazione effettuata con esperti legali; è anch'essa senza scopo di lucro e basata su volontari e riceve circa 50 segnalazioni alla settimana[65].

Il punto cruciale è comunque capire quale sia la reale possibilità del diritto di regolare in modo efficace il fenomeno o alternativamente affidare una parte della regolazione ad sistema, in questo caso al Cyberspace, prendendo spunto dalla sociologia sistemica di Niklas Luhmann. Nella sua sociologia sistemica non si parte dal riferimento all'azione individuale, ma piuttosto, al centro si trovano i meccanismi e i media di regolazione e controllo che appartengono ai singoli sub-sistemi entro il più ampio sistema sociale. Superata un'ottica metafisica, come egli definisce la filosofia occidentale basata sulla legge di causalità, viene alla luce la logica dei sistemi (politico, economico, morale), connotati da un loro peculiare medium (per esempio il potere o il denaro nel sistema politico o in quello economico)[66], mentre al pari, l'informazione potrebbe rappresentare il medium nel Cyberspace.

---

[61] Ibidem, pag. 2

[62] A questo proposito, un buon esempio viene dal Ministero della Giustizia Americano che attraverso l'ufficio "*Office of Justice and Delinquency Prevention's Missing and Exploited Children Program*" (MECP). Questo centro ha lo scopo di fornire copertura economica ad iniziative degli stati locali atte a creare risposte multi-giurisdizionali per prevenire e combattere crimini contro minori attraverso Internet.

[63] Sito WEB: http://www.cyberangels.org

[64] Vedi pagina 2 di "*State's Attorney and State Rep Lauren Beth Gash announce proposal to prohibit Cyberstalking*" ottenibile da http://www.statesattorney.org/aweb/prestak3.htm, copia del 24/04/2001.

[65] Si veda http://www.haltabuse.org/index.shtml acceduta il 2/05/2005.

[66] Gianluigi Palombella, "La conoscenza nell'interpretazione.Un modello per la giurisdizione", Democrazia e diritto, 1997

Ogni sistema è unico nel suo funzionamento, e chiuso a livello normativo: nel senso che esso replica alla complessità esterna, ambientale, e agli eventi che recepisce in termini di informazioni (attraverso un' "apertura cognitiva"); ma replica in base a proprie modalità autonomiche. Il sistema si autogoverna, non assume ordini dall'ambiente, e riproduce se stesso in base ai suoi stessi elementi (autopoiesi).

Ora, ciò significa quel che intuitivamente percepiamo: ossia che, ad esempio, il sistema economico non subisce causalisticamente al suo interno, come effetti necessitati, gli eventi che hanno luogo in un altro sistema, come quello politico; il sistema economico obbedisce comunque a propri imperativi anche nel trattare le contingenze esterne, le variabili ambientali, ed impedire che esse producano una diretta intrusione, una modificazione eteronoma nel sistema. Esso continua a seguire una sua logica di funzionamento, un suo equilibrio regolativo. Per questo, il sistema appare chiuso normativamente e aperto cognitivamente. Allo stesso modo il Cyberspace continua ad obbedire ai propri imperativi di anomia e di anonimia e sembra essere refrattario agli interventi regolativi del mondo reale.
Il diritto è inteso da Luhmann come una struttura che serve a ridurre la contingenza e l'esterna complessità che i sistemi devono fronteggiare. Essi possono durare se sono in grado di trasformare l'alta improbabilità di eventi in regolarità attendibili stabilizzando le aspettative; ruolo questo centrale per il diritto.
Sarebbe comunque riduttivo limitare il ruolo del diritto a quello di riduttore di complessità e stabilizzatore di aspettative in quanto diventa esso stesso un sistema capace di assicurarsi un'interna logica di funzionamento e imperativi propri, e condividere con gli altri sistemi le proprietà basilari, mantienendo un'apertura cognitiva e una chiusura normativa[67]. Il cyberspace può essere parimenti visto come qualcosa che non viene ordinato dall'esterno, ma in special modo prodotto e guidato da dinamiche interne.

Il sistema replica normativamente agli eventi acquisiti attraverso un'apertura cognitiva. E l'autoregolazione di un sistema come il Cyberspace deve apparire coerente con questa dinamica funzionale, porsi come ciò che sostanzia l'apertura cognitiva e permette la chiusura normativa.
La creazione e l'utilizzo di questi gruppi di supporto paralleli, che costantemente pattugliano il Cyberspace, aiutando le vittime di queste molestie e assicurando al sistema la "cattura" dei malintenzionati può essere vista come una componente di questa apertura cognitiva. E' interessante sottolineare che la cattura in questi termini si può manifestare in una natura diversa da quella del mondo reale. Il concetto di limitazione fisica che si esercita nel mondo reale con la limitazione della libertà fisica del malintenzionato, corrisponde nel Cyberspace alla perdita dell'anonimato della persona, alla scoperta della sua identità. E' questo l'elemento di passaggio tra l'elemento cognitivo aperto e quello normativo chiuso. Nel momento in cui l'identità del Cyberstalker è resa pubblica, esso può essere gestito in modo normativo abbandonando il sistema Cyberspace e rientrando in quello della società reale.

L'Inghilterra è una delle pochissime nazioni europee in cui sono state varate leggi (due) per contrastare il Cyberstalking[68]: il Protection from Harassment Act (1997) e il Malicious Communications Act (1998).

---

[67] Ibidem nota 66
[68] Si veda http://www.haltabuse.org/resources/laws/uk.shtml, acceduta il 12-05-2005

Invece, al momento, tutti gli Stati USA hanno legiferato una qualche forma di protezione e regolamentazione del fenomeno, ad eccezione di: District of Columbia, New Jersey, Utah, Nebraska, Idaho, e New Mexico (in corso). Comunque non è stata ancora approvata una legge federale sull'argomento[69].

Per quanto riguarda l'Italia, poco è stato fatto riguardo il Cyberstalking, mentre si sono avute importanti evoluzioni per gli altri Cybercrimini.
La 269/1998, *"Norme contro lo sfruttamento della prostituzione minorile, della pornografia minorile e del turismo sessuale a danno di minori quali nuove forme di riduzione in schiavitù"*, definisce la competenza della Polizia Postale per questa tipologia di reati.
La Polizia Postale è affiancata in questo compito dall' *Unità di Analisi del Crimine Informatico (UACI)* che è dotata di competenze tecnologiche, psicologiche e giuridiche; l'organismo ha anche un Comitato Scientifico di consulenza della Polizia Postale e delle Comunicazioni, i cui componenti sono professionalità di elevato valore dal mondo universitario ed ICT.

L'art. 14, comma 2 della stessa legge, ha dato strumenti nuovi per la lotta ai crimini perpetuati su Internet, come la possibilità di attivare siti civetta su Internet[70], effettuare degli acquisti simulati di materiale illegale[71] e partecipare ad interazioni elettroniche tramite mail e/o chat con la partecipazione alle stesse di agenti sotto copertura.
E' anche possibile intercettare le comunicazioni telematiche e duplicare la casella di posta utilizzata dall'indagato (permettendo la visione agli inquirenti della posta in arrivo, in partenza, ed in archivio)[72].

Sfortunatamente al di là di questi nuovi strumenti (validi sfortunatamente solo per una parte degli eventi criminali), c'è sempre la necessità di tracciare gli indirizzi IP tramite l'analisi dei files di log. Inizialmente resa impossibile dalla 675/1996 la tracciatura è di nuovo possibile; il problema è stato risolto con il T.U. 196/2003 sul trattamento dei dati personali, che ha introdotto una distinzione tra le finalità civilistiche e penali sulla conservazione dei dati da parte delle società di telecomunicazioni.
Non essendo comunque ancora tutto regolamentato, ha avuto ed ha un'importanza vitale la collaborazione che si è stabilita tra la Magistratura ed i gestori dei servizi di telecomunicazioni ed Internet.

---

[69] http://www.haltabuse.org/resources/laws/index.shtml, acceduta il 12-05-2005

[70] La generazione di siti civetta è un modo di successo per scoprire i pedofili. Attraverso un software che è in grado di simulare perfettamente l'identità e le interazioni di un bambino (tra gli 8 e i 13 anni) questa "esca virtuale" viene usata per intercettare eventuali molestie e/o tentativi di adescamento. Il software simula un atteggiamento caratterizzato da curiosità non eccessiva che convince l'addescatore a continuare la conversazione.

[71] Ad esempio, per scoprire chi realmente gestisce un sito di pedofili, gli agenti aprono un conto corrente intestato ad una persona fittizia, facendosi poi rilasciare una carta di credito con la quale acquistano il materiale illecito. A quel punto basta seguire il flusso di denaro per arrivare al beneficiario dell'operazione.

[72] L'intercettazione di comunicazioni informatiche e telematiche, previste dall'art. 266 bis c.p.p. così come introdotto dalla L. 547/1993, prevista per i procedimenti che si riferiscono ai reati indicati all'art. 266 c.p.p. a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche e per il reato previsto dall'art. 600 ter c.p., così come indicato dalla L. 269/98. L'intercettazione deve essere autorizzata dal P.M. e viene concessa solo quando vi sono gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini (fonte [Delle Donne.2004])

Se queste difficoltà non bastassero, occorre ricordare che questi fenomeni delittuosi sono connotati dalla rapidità e dalla tras-nazionalità delle attività. Anche se ciò ha comportato lo sviluppo di proficui rapporti collaborativi (metodologici ed operativi) con le pari organizzazioni presenti in altri Stati, la varietà delle configurazioni e degli accessi è tale, che questo rimane uno dei problemi più importanti da risolvere.

La definizione dei confini del Cyberstalking

Il primato di essere il primo Cyberstalker condannato dalle nuove leggi Californiane spetta a Gary S. Dellapenta, un uomo di 50 anni, ex guardia giurata, che e' stato messo in prigione nel 1999 con una pena di tre annni e con una cauzione di $300.000.

Dellapenta nutriva un interesse verso una donna di 28 anni che rifiutava le sue attenzioni. Utilizzò i mezzi informatici in modo da impersonare sulla rete la vittima, mandando messaggi su America On-line e nelle chat rooms per adulti. In questi messaggi il Dellapenta raccontava di essere una donna sessualmente insoddisfatta che aveva la segreta fantasia di essere violentata. Mise a disposizione il numero telefonico della vittima ed il suo indirizzo di casa e persino le istruzioni per disabilitare l'allarme di casa.

Fu l'inizio di un incubo per la donna: telefonate a tutte le ore e uomini che bussavano alla porta del suo appartamento di notte chiedendole di violentarla. Rivoltasi alla Polizia, dopo lunghe indagini l'uomo fu arrestato[73].

Il caso presenta vari aspetti interessanti. Per cominciare fu il primo caso in California che utilizzò l'estensione alla sezione *Civil Code § 1708.7 comma 2 e 3* che include il concetto di minaccia credibile (*credible threat*) utilizzando mezzi elettronici. Il caso destò quindi una grande attenzione sui media, favorendo l'attività di quanti negli altri Stati Americani stavano spingendo per l'adozione di norme simili.
L'impersonificazione della vittima è poi un altro elemento caratterizzante. Questo tipo di comportamento del molestatore è atipico in quanto questi rinuncia a quello che sembra essere il suo principale piacere: il controllo della vittima. Nel caso di impersonificazione, il controllo viene, infatti, delegato a terzi. Non si sa quanti raccoglieranno l'invito a molestare, ne quando questo avverrà.

L'eccitazione si muove dal controllo all'osservazione dello stato di disagio della vittima, presupponendo un'osservazione diretta della vittima che, in questo caso, non aveva mai posseduto un computer, e che non era quindi in grado neanche di capire quello che stava succedendogli intorno. Il caso evidenzia, infine, la necessità di regolamentazione delle attività degli ISP che sono fondamentali nell'identificazione dell'autore dei messaggi impersonificati.

Nel 1999 in Massachusetts ci fu un atteggiamento completamente diverso da parte delle istituzioni che si fecero trovare impreparate come contenuti professionali e come strumenti. "*Nanci*" iniziò a frequentare una chat room di tipo "romance" utilizzando un soprannome che

[73] Wired News, "Cyberstalking law invoked", 25 Gennaio 1999, da http://wired-vig.wired.com/news/politics/0,1283,17504,00.html, pagina acceduta il 2/05/2005

catturò l'attenzione di un altro frequentatore. La discussione si fece vivace in quanto il soprannome di Nanci non era gradito. La cosa non finì li. Tutte le volte che Nanci si collegava alla rete il molestatore la seguiva e diventava sempre più insistente ed aggressivo.

Iniziò a farle avere informazioni personali come il nome di suo padre, l'indirizzo di casa ed il suo numero telefonico, fino a minacciarla di morte. Terrorizzata Nanci si rivolse alla polizia locale, che le disse di spengere il computer, perché nient'altro poteva essere fatto. Il molestatore nel frattempo era diventato più aggressivo mandando messaggi di posta elettronica, messaggi istantanei tipo ICQ, dicendogli il tipo di macchina che guidava ed il numero della targa, il nome della figlia, dove fosse stata qualche minuto prima, e cose similari.
Nanci andò dalla polizia di stato, dal county *District Attorney*, e alla fine dallo *State Attorney General*. Nessuno si mosse, puntando l'un l'altro la responsabilità dell'intervento.
A quel punto Naci ingaggiò un avvocato e fece una denuncia contro ignoti per molestie fisiche presentandosi in aula con giornalisti e televisione. A quel punto il District Attorney decise di aiutarla ed il molestatore fu imputato di reato[74].

Il Massachussetts ha oggi regolamentato il Cyberstalking sotto il Chapter 265: Section 43[75]. Casi come questo sono molto meno rari di quello che si pensi. Soprattutto nel periodo 1998-2000, prima cioè che la spinta dei media e dei cittadini obbligasse il legislatore a prendere sul serio il fenomeno, l'atteggiamento delle istituzioni di controllo era quello di ignorare le vittime, considerando il problema quasi come un litigio tra adolescenti per cause di gioco.
I primi assassinii, cioè i primi casi di Cyberstalking trasformatisi in crimini tradizionali, montarono un'attenzione dei media talmente grande da rendere impossibile per le istituzioni di ignorare il fenomeno ulteriormente.

Uno dei primissimi casi di omicido con connessione al Cyberstalking fu probabilmente quello che vide per vittima Rebecca Schaeffer, attrice, uccisa nel suo appartamento di Hollywood nel Luglio del 1989. L'assassino John Bardo, con delle scuse le fece aprire la porta e le disse, trovando il coraggio, che era un suo grande ammiratore e che avrebbe voluto entrare in casa per parlare con lei. La donna non aveva mai visto quell'individuo ed allarmata che conoscesse chi fosse e dove abitasse, gentilmente rifiutò di farlo entrare.

Dopo pochi minuti l'uomo con un altro stratagemma si fece aprire di nuovo uccidendo l'attrice con un colpo di pistola in pieno petto. Le indagini successive scoprirono che la donna era stata molestata da questo individuo da lungo tempo. Anche se i due vivevano in posti distanti, Bardo la seguiva in modo costante. Sapeva tutto di lei attraverso il computer. Le sue proprietà, cosa mangiava, cosa comprava, la macchina che guidava, numeri telefonici, carte di credito ed altro[76].

Questo caso e' simile a quello di Dellapenta in quanto la vittima non era una frequentatrice del Cyberspace, e si identifica bene nella casistica del Cyberstalker di tipo sognatore che e' stato descritto in precedenza. La vittima, una celebrità, ha catturato l'attenzione del molestatore suo malgrado e non era a conoscenza di essere tracciata fino al momento dell'aggressione fatale.

---

[74] J.A. Hitchcock, "Cyberstalking", Agosto 2000, disponibile su http://www.netcrimes.net/medialist.html, acceduto il 2-05-2005
[75] Vedi **Errore. L'origine riferimento non è stata trovata.** a pagina **Errore. Il segnalibro non è definito.**
[76] Jessica Laughren, "Cyberstalking Awarness and Education", 1999, ottenibile da http://www.acs.ucalgary.ca/^dabrent/webproj/jessica.html, copia del 30/04/2001.

Si consideri anche che si sta parlando del 1989, anno in cui il numero di informazioni presenti on-line riguardo tutti noi era di vari ordini di grandezza inferiore a quella di oggi.

A seguito di questo incidente, la California fu il primo stato americano a legiferare in merito di Stalking (1990); questa attenzione allo stalking, forzata anche dalla presenza in questo stato di una forte concentrazione di persone celebri e di persone con alte conoscenze informatiche portò lo stato a legiferare sul Cyberstalking nel 1999.

Nell'ottobre del 1999 una ragazza di 20 anni, assistente in uno studio, fu uccisa all'uscita del suo posto di lavoro da Liam Youens, 21, che poi si suicidò. Apparentemente la vittima e l'assassino non avevano connessioni e la polizia faticò non poco prima di trovarne. La svolta investigativa avvenne quando la polizia sequestrò il computer del giovane assassino. Il giovane frequentava la stessa scuola della vittima.
Non si conoscevano, ma lui si infatuò terribilmente fino a generare odio quando la vide in compagnia del suo fidanzato. Liam perse poi le tracce della ragazza, ma mantenne il suo amore odio, dedicando a lei due WEB site con accluso un diario delirante su cui alternativamente annotava i suoi idilli o i suoi messaggi di odio. Ma non riusciva a rintracciare la ragazza nonostante avesse apposto su internet anche sue fotografie. L'imprevedibile avvenne quando la ragazza si collegò su internet per prenotare un viaggio, ignara del suo destino.
L'intercettazione fu immediata e tre giorni dopo era morta[77]. Questo tipo di Cyberstalking sarà difficilmente regolamentabile, e le forze di controllo difficilmente riusciranno a prevenire crimini come questi. L'unico rimedio appare una risposta dell'industria atta a proteggere meglio le informazioni e a tutelare gli utenti di internet che operano su di essa.

Un caso interessante per il modo in cui la corte si e' comportata, e che potrebbe essere usata come esempio per il futuro, e' quello che ha visto la *Internet America Inc*. vs *Kevin Massey* nel 1997. La Internet America Inc. e' un Internet Service Provider in Dallas. Massey continuamente mandava messaggi di minaccia ed insulti di vario genere su USNET al CEO della società e a sua moglie. Quest'ultima ebbe importanti problemi emotivi derivanti dalle minacce.
Le minacce, in questo caso di danni fisici, furono estese anche ai dipendenti della società. Dal momento che non era possibile fermare il Massey nonostante le diverse richieste, il Giudice Joe B. Brown emise un'ordinanza di fermo per on-line harassment. Data l'urgenza del caso, il Giudice decise di utilizzare lo stesso mezzo informatico usato dal molestatore e gli comunicò l'ingiunzione per e-mail invece che per i canali ufficiali[78].

Il problema del "True Threats"

Negli USA la libertà di espressione e' protetta dal cosiddetto primo emendamento (*First Amendment*). Un problema molto importante che accompagna tutte le discussioni relative al Cyberstalking e' la definizione di quello che viene chiamato il "*true threat*", cioè quale deve essere la metodologia per definire una minaccia che sia veramente tale. Solo in queste condizioni la minaccia può essere considerata reato senza violare la Costituzione. Nel passato ci sono state parecchie controversie in relazione alla metodologie utilizzate per validare un *true*

[77] Ibidem nota 74
[78] Marie D'amico, "The law vs. online stalking", feb 1997, da http://lawcrawler.findlaw.com/MAD/cybersta.htm, pagina acceduta il 2/05/2005

threat, ma negli ultimi 25 la discussione si era stabilizzata intorno ad alcuni casi modello che venivano utilizzati come precedenti legali.

Una delle tecniche più utilizzate dalle corti nel passato per il test di validità di una *true threat* e' la cosiddetta "*objective construction*"[79]. Con questa tecnica in pratica ci si chiede se una persona ragionevole avrebbe interpretato il discorso in analisi come una minaccia, dato il contesto in cui il discorso stesso fu fatto.
Il punto su cui le corti tipicamente si differenziano è chi dovrebbe essere questa persona ragionevole; ci sono tre possibilità:

A) chiedersi se un ascoltatore indipendente dalle minacce, ascoltando la dichiarazione la consideri una minaccia
B) chiedersi se una persona ragionevole avrebbe potuto immaginare che tale dichiarazione si sarebbe potuta interpretare come minaccia
C) chiedersi se una persona ragionevole oggetto di tale dichiarazione l'avrebbe potuta considerare come una minaccia

Queste tecniche, specialmente la A e C, sono molto soggettive, e dipendono dal livello di sensibilità delle persone sottoposte al test. Il pericolo e' che una dichiarazione venga considerata una minaccia solo perché il ricevente aveva una sensibilità troppo elevata. Per eliminare questo inconveniente alcune corti hanno introdotto un test di tipo "*subjective*" che in pratica si domanda:

- se chi ha fatto la dichiarazione avesse l'intenzione di minacciare
- se chi ha fatto la dichiarazione avesse l'intenzione di eseguire la minaccia

L'esplosione del fenomeno del Cyberstalking e del Cyberspace più in generale ha riproposto il problema con rinnovato interesse: tenere sotto controllo il fenomeno del Cyberstalking senza per questo operare ingiustificate censure e mantenere attiva la protezione per la libertà di parola.

Si rende sicuramente necessario definire un test che elimini quanto possibile il problema della limitazione della libertà di espressione, limitando l'influenza delle diverse sensibilità delle persone che saranno poste di fronte al test stesso, ma ad oggi la ricerca effettuata non ha evidenziato nessun caso legale che abbia riproposto negli USA la questione in modo esaustivo.

Per dare un'idea dell'importanza del *true threat* nelle questioni di Cyberstalking, presenterò di seguito due casi diversi che hanno visto un uso differente della posta elettronica per esercitare delle minacce, vedendo come nel primo caso non siano state considerate valide le imputazioni (nonostante la gravità del linguaggio utilizzato) mentre nel secondo caso si.

Il caso United States v. Jake BaKer[80]

---

[79] Anna S. Andrews, "a proposed true threats test to safeguard free speech rights in the age of internet", May 1999, the UCLA Online Institute for Cyberspace Law and Policy, ottenibile da http://www.gseis.ucla.edu/iclp/aandrews2.htm, pagina acceduta il 05/05/2005.
[80] Il testo della sentenza di primo grado e' riportato in Allegato

Abraham Jacop Alkhabaz, uno studente dell'Università del Michigan, conosciuto anche con lo pseudonimo di Jake Baker, scambiò più di 40 messaggi di posta elettronica con un personaggio la cui vera identità non fu mai scoperta, ma riportato negli atti come Arthur Gonda. Lo scambio di messaggi avvenne tra il novembre 1994 e il Gennaio del 1995. Il contenuto di questi messaggi era esplicitamente di natura sessuale violenta. In pratica i due si scambiavano storie e proposte su come violentare, torturare ed assassinare una compagna di corso di Jake Baker.

Un agente dell'FBI intercettò una storia mandata da Baker ad un newsgroup ("*alt.sex.stories*") e di li scattarono una serie di intercettazioni che produssero i messaggi di posta elettronica di cui all'accusa. Backer fu arrestato nel Febbraio del 1995 e fu rilasciato su cauzione dopo che una visita psichiatrica dimostrò che non era pericoloso per la società. Più tardi il Procuratore incriminò Backer con 5 capi di accusa per violazione del 18 U.S.C. § 875(c).

Il 18 U.S.C. § 875(c) afferma che chiunque invii in un'attività commerciale, tra stati US o nazioni straniere, qualsiasi comunicazione contenente qualsiasi minaccia di sequestrare o qualsiasi minaccia di ferire un'altra persona deve essere sanzionato secondo quest'articolo o imprigionato per non più di 5 anni, o entrambe le cose.

Gli investigatori ed il Procuratore avevano la convinzione che i due si stessero scambiando all'inizio delle fantasie, ma che con l'andar del tempo queste stessero assumendo le sembianze di un piano preciso per le azioni delittuose descritte. Il procuratore fu in grado di provare i tre termini necessari all'incriminazione sotto il 18 U.S.C. § 875(c):

- trasmissione tra stati
- comunicazione contente una minaccia
- la minaccia deve essere quella di sequestrare o ferire un'altra persona

ma in ben due gradi di giudizio, le accuse furono fatte cadere.

La corte distrettuale, *The District Court*, dichiarò che i messaggi di posta elettronica erano privati e che non c'era evidenza di intenzioni di distribuirli ad altre persone, meno che mai alla ragazza oggetto delle minacce. A quel punto per essere una minaccia, il messaggio lo sarebbe dovuto essere per Arthur Gonda, il quale invece mostrava di apprezzarle e di non interpretarle come minaccia. Inoltre nei messaggi non si faceva esplicito riferimento ad una ragazza in particolare, ma si usavano appellativi, che, anche se insultanti, non identificavano chiaramente la vittima, condizione questa fondamentale per l'articolo in questione. Chi ricorse contro l'applicazione del 18 U.S.C. § 875(c) in questa causa fu l'*American Civil Liberties Union's (ACLU)*[81].
La corte di appello (*The court of Appeals)*, fece anch'essa cadere le accuse utilizzando però motivazioni diverse. In pratica affermò che i messaggi di posta elettronica non rappresentavano una *true threat* e di conseguenza erano protetti dal principio di libertà d'espressione sancito dal primo emendamento. La motivazione dietro quest'affermazione e' che la corte intese la minaccia come uno strumento di intimidazione per ottenere qualcosa da qualcuno: la minaccia ha senso se e solo se il molestatore ha uno scopo e la minaccia serve a raggiungerlo.

---

[81] U.S. vs Jake Baker & Arthur Gonda, ottenibile da http://www.mit.edu/activities/safe/cases/umich-baker-story/ copia del 3-05-2005. Utile la lettura di http://csethics.uis.edu/dolce/teachAids/JHuggins.html, copia del 3-05-2005. Si veda anche un caso simile Watts v U.S. .

In realtà la corte si divise nel raggiungere il verdetto, con il giudice Krupansky in minoranza che non condivideva le modalità con cui era stato deciso il decadere delle accuse.

Il caso della Woodside Agency[82]

La storia comincia nel 1996, quando un'innocente annuncio venne pubblicato sul newsgroup *misc.writing* e su *rec.arts.books.childrens*. L'annuncio era di un agente letterario che diceva di cercare promettenti scrittori per degli editori e diceva:

> Subject: WRITERS SEEKING PUBLICATION
> From: CFSQ98A@prodigy.com (James Leonard)
> Date: 1996/01/24
> Newsgroups: rec.arts.books.childrens
> The Woodside Literary Agency is now accepting new authors, re: fiction and non fiction: children's books. Advances from publishers can be high. You must have a completed manuscript. We have offices from New York to Florida. Email for information: CFSQ98A@prodigy.com. If you respond during the month of February, call my new Florida agency at: xxx-xxx-xxxx.
> I will be there in February.
> James

L'annuncio, che comunque era stato pubblicano in un newsgroup non opportuno[83] catturò l'attenzione di Jayne Hitchcock[84] la quale prima chiamò l'agenzia al telefono e poi le inviò un manoscritto. Dopo qualche giorno ricevette una risposta contente una proposta di uso professionale dell'agenzia con un onorario di $75. Jayne, sapeva che non era un comportmanto corretto per un agente letterario, in quanto l'*Association of Authors' Representative* vieta di chiedere onorari per queste prestazioni.

Scrisse all'agenzia dicendo che la richiesta di onorario non era stata precisata nell'annuncio e che non era dovuta. Dopo poco ebbe indietro il manoscritto. Passate poche settimane, la Woodside cominciò a mettere annunci su *misc.writing*. Nonostante gli aspiranti scrittori mandassero i peggiori lavori a proposito, l'agenzia era sempre d'accordo con la pubblicazione e richiedeva un onorario che ora era diventato di $150.

La Jayne cominciò così ad investigare sull'attività della Woodside e cominciò a distribuire messaggi sui newsgroups per avvertire gli aspiranti scrittori del comportamento scorretto dell'agenzia. A quel punto la Woodside cominciò un'attività di danneggiamento sistematico dell'utenza della Jayne[85]. Divennero oggetto degli attacchi anche il newsgroup stesso ed altri componenti del gruppo che avevano aiutato la Jayne nelle denuncie.

---

[82] Si veda "
Chiamata in giudizio del caso Woodside " a pagina 47 e "
Sentenza di Abdus-Salaam sul caso Woodside" a pagina 51
[83] Non e' consentito pubblicare annunci commerciali in questi newsgroup
[84] Jayne è oggi Presidente dell'organizzazione "Working to Halt Online Abuse" WHO@.
[85] Tecnicamente chiamato *spam*. Furono inviate anche parecchie *mail-bombing*, mail molto grandi che servono a far andare in errore le applicazioni del ricevente

Vennero messi annunci in cui la Jayne si dichiarava disponibile a fantasie sessuali e a condividerle con frequentatori occasionali. Vennero pubblicati il suo indirizzo ed il suo numero di casa. Gli vennero anche fatti abbonamenti a riviste non richiesti. La polizia locale, e l'FBI non furono in grado di aiutarla, cosi con degli amici si mise a ricercare i Cyberstalkers fino ad identificarli. A quel punto, aiutata da un avvocato, la Jayne fece causa contro la Woodside, chiedendo inizialmente un risarcimento di 10 Milioni di dollari[86].

Nel Febbraio del 1999 il procuratore generale Eliot Spitzer annunciò che la Woodside era stata condannata ad interrompere la sua pratica su Internet e a rifondere tutte le sue vittime oltre al pagamento delle spese processuali. Nonostante questo gli attacchi non terminarono e gli autori del Cyberstalking furono arrestati dalla polizia postale di New York nel Gennaio 2000.

Questo caso e' evidentemente diverso dal precedente, anche se ugualmente basato su messaggi di posta elettronica. Prima di tutto non vi era un rapporto privato tra due come nel caso di Baker, ma non vi era neanche una diretta minaccia dei proprietari della Woodside alla Jayne. Il caso ricorda un po' quello di Dellapenta, con l'utilizzo dei mezzi elettronici a fine di creare uno stato di angoscia ed ansia nella vittima. In questo caso la minaccia era identificata anche nello scopo, che era quello di vendicarsi dell'attività investigativa svolta dalla Jayne.

Un caso particolare di Cyberstalking: lo stupro virtuale

I Multiple User Dungeons sono meglio conosciuti come MUD[87]. Inizialmente nati come giochi di ruolo virtuali si sono evoluti fino a comprendere ambienti sociali di solidarietà ed ambienti didattici. Il sesso e' una delle componenti fondamentali nei MUD ed avviene inviandosi tra due o più giocatori la descrizione di atti fisici ed emotivi.

La riflessione che vorrei fare su questo ambiente, apparentemente privo di regole, è legato ad un episodio che creò un certo scalpore in uno dei MUD storici, il LambdaMOO.

All'interno di un MUD possono accadere episodi di stupro virtuale quando un partecipante trova un'alchimia tecnica (bambola Woodoo) per prendere il controllo di un altro personaggio costringendolo ad avere un rapporto sessuale indipendentemente dalla volontà del proprietario del personaggio.

Fu quello che accadde allorché un personaggio di nome Mr. Jungle prese il controllo di un personaggio femminile di nome Legba, costringendola ad avere un rapporto sessuale non consenziente. Legba si rivolse alla mailing list per gli affari sociali del MUD, lista che in pratica rappresentava una sorta di auto-governo del MUD. Il problema fu argomento di discussioni accese su come si dovesse considerare quel fatto e se esso potesse essere considerato un reato, perseguibile nel MUD ed anche nella vita reale.

---

[86] Si veda http://members.tripod.com/~cyberstalked/complaint.html acceduta il 6-05-2005 e http://www.unc.edu/courses/pre2000fall/law357c/cyberprojects/spring00 acceduta il 4-05-2005.

[87] Per saperne di più sui MUD si può partire dal sito http://www.mud.it/elencomud.php.

I MUD in genere e LambdaMOO in particolare hanno un sistema per incoraggiare i giocatori a seguire le regole interne.

Esistono comandi come il "*gag*" che consente di imbavagliare un partecipante che molesta o che è troppo di distrurbo agli altri. Una punizione più grave è il "toading", termine originale inventato dai costruttori dei primi MUD. Consente di trasformare le sembianze di un giocatore fino a farlo diventare un ripugnate rospo[88], ma nel tempo ha assunto il significato di una terminazione del personaggio, che può essere chiesta per votazione dagli altri partecipanti.

Quindi anche i MUD hanno le loro convenzioni sociali, con i giocatori che delegano alcune libertà alle autorità di controllo, i "wizard", per vivere in un mondo prevedibile. Come si diceva nel paragrafo precedente, viene definito una sorta di diritto che nella normatività estrinseca crea l'aspettativa di stabilità della struttura sociale su cui si pone.

Thomas Hobbes ha proposto il concetto di Leviatano definito come " il Dio mortale al quale dobbiamo obbedire dopo il Dio immortale; la nostra pace e la nostra difesa"[89]. Il Leviatano potrebbe essere interpretato come un sistema di governo al quale affidiamo il potere di dirimere le controversie oppure ad un personaggio di un particolare potere, con potere di vita e di morte sulla sua popolazione. In pratica i Mud hanno scelto una via intermedia tra le due posizioni.

Il Leviatano è interpretato dalla figura del wizard (mago), mentre esiste un piccolo governo, auto-eletto, che ha il potere di eleggere i Wizard e di decidere in merito a questioni importanti come l'esecuzione di pene di toading. I Wizard devono essere visti come dei moderatori, con il compito ad esempio di censurare messaggi non pubblicabili, e la presenza di questa moderazione tranquillizza i partecipanti.

Fu proprio il LambdaMOO comunque testimone di una situazione molto interessante. All'inizio nel MOO i Widzard avevamo potere assoluto. Nel 1992 Pavel Curtis, fondatore ed inventore del MOO, inviò alla mailing list degli affari sociali un messaggio in cui i magi abdicavano il potere ad un organo di autocontrollo[90]. Il problema fu che Curtis non definì quale quest'organo dovesse essere e la comunità del LambdaMOO non se lo autodefinì. I giocatori cominciarono a litigare fra di loro e la comunità cominciò a disgregarsi.

Il punto culminante ci fu quando avvenne il caso di Cyberstupro di cui abbiamo parlato; l'indignazione dei partecipanti montò e ci fu quasi il rischio di una seria instabilità, fino a quando un mago si assunse la responsabilità di effettuare un toading del personaggio colpevole dello stupro. Occorre ricordare che un giocatore ha una vera e propria esistenza in un MUD. Impiega giorni e giorni di connessione per fare amicizie, per costruirsi la propria abitazione, per crescere nella scala sociale. Se per qualunque motivo l'identità del personaggio viene danneggiata, il danno e' notevole, e molte volte crea situazioni di ansia nella persona fisica non dissimili da quelle ingenerate dal Cyberstalking.

---

[88] Ibidem nota **Errore. Il segnalibro non è definito.**, pagina 95
[89] Ibidem nota **Errore. Il segnalibro non è definito.**, pagine 96-99
[90] P. Curtis, "not just a game: how Lambda came to exist and what it did to get back at me", 1997, http://www.cs.unm.edu/~raybourn/moo5d~1.htm acceduta il 30-04-2005, http://www.g4tv.com/techtvvault/features/38666/The_Incredible_Tale_of_LambdaMOO.html acceduta il 2-05-2005.

Dopo questa esperienza Curtis definì un processo di petizione formale ispirato al processo di iniziativa popolare in California. Anche questa esperienza fallì in seguito a causa del disinteressamento dei partecipanti a seguire la carriera politica, una sorta di apatia simile a quella che si riscontra nella vita sociale reale. Fu così che nel 1996 Curtis reintegrò i maghi come leviatano.

Spunti di ricerca sul Cyberstalking

Sicuramente il fenomeno ha attirato l'attenzione dei media per qualche fatto criminoso, contribuendo a formarne un'idea nell'immaginario collettivo che potrebbe essere ben diversa dalla realtà.
Diventa quindi urgente **(1)** poter contare su un impianto teorico corretto che percorra i vari paradigmi interpretativi del comportamento deviante, da quello utilitaristico a quello positivistico, da quello interazionista a quello conflittuale, posizionandovi il fenomeno del Cyberstalking e capendo quale tra questi sia il migliore candidato per la sua epistemiologia.

Marco Strano asserisce che *<<Alcune azioni eclatanti condotte da parte di soggetti solitari e disorganizzati (es. i giovani hackers) riescono, grazie al funzionamento delle reti, ad "attaccare" i gangli vitali della società moderna. Si tratta spesso di comportamenti criminali dove la dimensione "espressiva" assume un ruolo primario rispetto a quella pragmatico-utilitaristica;>>*[91]. Una possibile analisi **(2)** potrebbe studiare il contenuto "ideologico" di questi atti delittuosi che, rifiutando una genesi utilitaristica, possano avere una familiarità con gruppi politici e religiosi che potrebbero sfociare anche in rappresentazioni integraliste ed estremistiche. Un'ulteriore approfondimento **(3)** potrebbe riguardare il blurring tra la percezione ludica che spesso hanno questi attori e l'agire in modo deviato.

Da un punto di vista degli attributi biologici del molestatore, si potrebbe studiare: **(4)** perché le persone più adulte tendono più degli adolescenti a perpetuare reati di Cyberstalking; **(5)** l'evoluzione del genere femminile nel ruolo di aggressore e approfondire l'incremento di frequenza che si è verificato negli ultimi anni.

Leggendo poi una correlazione tra il mondo reale e quello virtuale nei fatti delittuosi, si potrebbe analizzare **(6)** la recidività tra gli autori di Cybercrime in relazione a precedenti reati commessi nei modi tradizionali.

Altri spunti emersi sono:
(7) Analisi di quali comportamenti fanno si che la vittima sia selezionata come tale dal molestatore.
(8) Analisi della relazione tra lo skill informatico (sia del molestatore che della vittima) e la tipologia di crimine perpetuato.
(9) Analisi delle implicazioni psicologico/comportamentali sulla vittima dei casi di sostituzione di identità.
(10) Capire se nel caso di "informatizzazione" dei crimini tradizionali, gli attori devianti sono stati sottoposti alle stesse influenze sociali di quelle tradizionali e se le due tipologie di crimine sono perpetuate contemporaneamente.

---

[91] Marco Strano, "Dal cyberfuturismo al cybercrime: la spiegazione del comportamento criminale connesso alla tecnologia digitale", 2003, ottenibile da http://www.poliziadistato.it/pds/informatica/allegati/cyberfoturismo.pdf copia del 28/04/2005

(11) Analizzare il corpo normativo vigente sulle minacce e le aggressioni off-line, capendo quali differenze si possono ravvisare rispetto a quelle on-line, in modo da proporre un percorso di avvicinamento annullando la differenza legislativa tra Cybercrime e crimini tradizionali.
(12) Analizzare le possibili evoluzioni della L. 196/2003 (Privacy) in relazione al fenomeno del Cyberstalking e delle necessità investigative presso ISP e fornitori di servizi informatici.

Riferimenti bibliografici

Aclu 2000	U.S. vs Jake Baker & Arthur Gonda, ottenibile da http://www.mit.edu/activities/safe/cases/umich-baker-story/ copia del 3-05-2005.
Andrews 1999	Anna S. Andrews, “a proposed true threats test to safeguard free speech rights in the age of internet”, May 1999, the UCLA On-line Institute for Cyberspace Law and Policy, ottenibile da http://www.gseis.ucla.edu/iclp/aandrews2.htm, pagina acceduta il 05/05/2005.
Asch 1946	Salomon E. Asch, “Forming Impression of personality”, In Journal of Abnormal and Social Psychology, 1946
Barandes 1999	Laura Barandes ,”Focus on New York’s Rape Shiled Law”, Court TV, 22 Dicembre 1999, ottenibile da HTTP://www.courttv.com/national/1999/1223/jovanovic_ctv.html, pagina acceduta il 22/04/2005.
Berzano 1998	Luigi Barzano e Franco Prina, “Sociologia della devianza”, 1998, Carocci Editore, ISBN 88-430-0325-9
Canetti 1997	Elias Canetti, “Massa e potere”, Biblioteca Adelfi, 1997
Curtis 1997	P. Curtis, “not just a game: how Lambda came to exist and what it did to get back at me”, 1997, oppure http://www.cs.unm.edu/~raybourn/moo5d~1.htm acceduta il 30-04-2005, http://www.g4tv.com/techtvvault/features/38666/The_Incredible_Tale_of_LambdaMOO.html acceduta il 2-05-2005.
Cyberguards	“What Is Cyberstalking? From the U.S. Department of Justice”, CyberGuards, ottenibile da http://www.cyberguards.com/CyberStalking.html, referenza acceduta il 30/04/2005
D'Amico 1997	Marie D’amico, “The law vs. on-line stalking”, feb 1997, da http://lawcrawler.findlaw.com/MAD/cybersta.htm, pagina acceduta il 2/05/2005
Davis 1996	Jim Davis, CNET News, “Stalker’s home page scares Banyan”, June 1996, ottenibile da http://news.com.com/2100-1023-215869.html?legacy=cnet, acceduta il 2/05/2005.
Delle Donne 2004	Monica delle Donne, “Tecniche di indagine nell’ambito dei reati informatici”, 2004, Diritto&Diritti, copia del 10-05-2005, ottenibile da http ://www. diritto. it/articoli/dir tecnologie/delle donne.html
Gash 2001	“State’s Attorney and State Rep Lauren Beth Gash announce proposal to prohibit Cyberstalking” ottenibile da http://www.statesattorney.org/aweb/prestak3.htm, pagina acceduta il 30/04/2001
Granieri 2005	Giuseppe Granieri, “Blog Generation”, 2005, Editori Laterza, ISBN 88-420-7564-7
Hitchcok 2000	J.A. Hitchcock, “Cyberstalking”, Agosto 2000, disponibile su http://www.netcrimes.net/medialist.html, acceduto il 2-05-2005
Laughren 1999	Jessica Laughren, “Cyberstalking Awarness and Education”, 1999, ottenibile da http://www.acs.ucalgary.ca/^dabrent/webproj/jessica.html, pagina acceduta il 30/04/2001.
Mari 2004	Alberto Mari, “Web publishing con Blog e Wiki”, 2004, Apogeo, ISBN 88-503-2292-5

Palombella 1997	Gianluigi Palombella, “La conoscenza nell'interpretazione.Un modello per la giurisdizione”, Democrazia e diritto, 1997
Strano 2002	Marco Strano, “Nuove tecnologie e nuove forme criminali”, 2002, Cybercrime International Conference, ottenibile da http ://www.poliziadistato . it/pds/primapagina/cybercrime/index.html copia del 10-05-2005
Strano 2003	Marco Strano, “Dal cyberfuturismo al cybercrime: la spiegazione del comportamento criminale connesso alla tecnologia digitale”, 2003, ottenibile da http://www.poliziadistato.it/pds/informatica/allegati/cyberfoturismo.pdf copia del 28/04/2005
Unc 2000	“Cyberstalking Cases” ottenibile da: http://members.tripod.com/~cyberstalked/complaint.html acceduta il 6-05-2005 e http://www.unc.edu/courses/pre2000fall/law357c/cyberprojects/spring00 acceduta il 4-05-2005.
Usdoj-01 2001	“Report on Cyberstalking: a New Challenge for Law Enforcement and Industry; A Report from the Attorney General to the Vice President Al Gore”, 1999, disponibile su http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm, pagina acceduta il 24/04/2005.
Usdoj-02 2001	“OVC Resource Center and the National Criminal Justice Reference Service (NCJRS) 2001 report” ottenibile dal sito del Ministero della Giustizia Americano, http://www.usdoj.gov
Usdoj 1998	“Stalking in America”, risultati sull'indagine effettuata dal National Violence Against Women, US Department of Justice, Office of Justice Programs, and Departments of Health and Human Services, Center of Desease and prevention, April 1998, ottenibile da http://www.usdoj.gov/ojp
Wallace 2000	Patricia Wallace, “La psicologia di internet”, Raffaello Cortina Editore, 2000, pg. 20-22
Wired 1999	Wired News, “Cyberstalking law invoked”, 25 Gennaio 1999, da http://www.wired.com/politics/0,1283,17504,00.html, pagina acceduta il 22/04/2001

Altre sorgenti utili per la tematica trattata

- Corsi on-line (1998), *La sicurezza in Internet*, in http:// www.provincia.si.it/ corsi/ la_sicurezza_in_internet/lll.html .
- http://www.crimelibrary.com/criminology/cyberstalking
- Utile la lettura di http://csethics.uis.edu/dolce/teachAids/JHuggins.html
- Damiani E. (1998)*, Agenti intelligenti*, in www.tecnet.it/articoli/
- Databank Consulting (1995), *Rapporto sul mercato dei servizi Internet e Intranet*, in http://www.databank.it/ dbk/ databank.htm
- Datamonitor (1997), *E-commerce*, in http://www.datamonitor.com .
- Giano F. (1998), *Schede*, in http://www.uinve.it/%7egiano/diritto_commerciale/ schede/ sla22400.htm.

- Mandelli A. (1996), *Internet e new media: comunicazione di massa per il marketing relazionale*, in http://www.tin.it/osservatorio_bocconi/paper18.htm, Progetto Media & New Media, Osservatorio di Marketing, SDA Bocconi.
- Mandelli A. (1997a), *Internet e il commercio elettronico: metafore di aggregazione e nuovi intermediari*, in http://www.tin.it/osservatorio_bocconi/papercomm.htm, Progetto Media & New Media, Osservatorio di Marketing, SDA Bocconi.
- Mandelli A. (1997b), *Il commercio elettronico in Internet: natura e dimensioni del fenomeno nel mondo e in Italia*, in http://www.tin.it/ osservatorio_bocconi/ ecomm.htm, Università Bocconi Milano & Indiana University Bloomington (IN).
- OCSE (1996), *Guidelines*, in http://www.oecd.org/dsti/iccp/crypto-e.html.
- Wall Street Journal (1997), *Special Report: on-line trading*, in http://interactive .wsj.com/ public/ resources/ documents/ on-line98-cover.htm
- Wladawski I. (1998), *Intervista*, in http:// www.mediamente.rai.it/ home/ bibliote/ intervis/ w/ wladawski.htm.
- Zimmerman O. (1998), *Structural and managerial aspects of virtual enterprices*, in http://www.tin.it/osservatorio_bocconi/,
- Virtuelle Bocij, P., 2002. "Corporate cyberstalking: an invitation to build theory". First Monday, 7 (11) http://firstmonday.org/issues/issue7_11/bocij/index.html.
- Bradley, N., 1999. "Sampling for Internet Surveys: An examination of respondent selection for Internet research". http://users.wmin.ac.uk/~bradlen/papers/sam06.html
- Indirizzi Internet di organizzazioni che si occupano di Cyberstalking:

  http://www.ed.gov

  Safeguarding Our Children United Mothers: http://www.soc-um.org

  Safe Kids: http://www.safekids.com

  Kid Safe: http://www.kidsafe.com

  Child Safety on the Information Highway: http://www.4j.lane.edu/safety/childtoc.html

  http://www.childrenspartnership.org

  FBI: http://www.FBI.gov

  CyberGuards: http://www.cyberguards.org

  Cyberangels: http://www.cyberangels.org

Allegati

Sentenza di A. Cohn in U.S. vs J. Baker

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. Criminal No. 95-80106 Honorable Avern Cohn
JAKE BAKER and ARTHUR GONDA, Defendants.

OPINION

> "It is not the policy of the law to punish those unsuccessful threats which it is not presumed would terrify ordinary persons excessively; and there is so much opportunity for magnifying or misunderstanding undefined menaces that probably as much mischief would be caused by letting them be prosecuted as by refraining from it."

The People v. B. F. Jones, 62 Mich. 304 (1886).

I. Introduction

This is a criminal prosecution under 18 U.S.C. ¤ 875(c). Defendant Jake Baker (Baker) is charged in a superseding indictment with five counts of transmitting threats to injure or kidnap another, in electronic mail (e-mail) messages transmitted via the Internet.[1] Now before the Court is Baker's motion to quash the superseding indictment.[2] For the reasons that follow, the motion will be granted.

II. Background

The e-mail messages that form the basis of the charges in this case were exchanged in December, 1994 between Baker in Ann Arbor, Michigan, and defendant Arthur Gonda (Gonda), who sent and received e-mail through a computer in Ontario, Canada. Gonda's identity and whereabouts are unknown. The messages excerpted in the superseding indictment are drawn from a larger e-mail exchange between Gonda and Baker began on November 29, 1994, and ended on January 25, 1995. The specific language of the messages excerpted in the superseding indictment will be discussed in detail below. They all express a sexual interest in violence against women and girls.

Baker first appeared before a United States Magistrate Judge on a criminal complaint alleging violation of 18 U.S.C. ¤ 875(c), on February 9, 1995. The complaint was based on an FBI agent's affidavit which cited language taken from a story Baker posted to an Internet newsgroup entitled "alt.sex.stories," and from e-mail messages he sent to Gonda. The story graphically described the torture, rape, and murder of a woman who was given the name of a classmate of Baker's at the University of Michigan. The "alt.sex.stories" newsgroup to which Baker's story was posted is an electronic bulletin board, the contents of which are publicly available via the Internet. Much of the attention this case garnered centered on Baker's use of a real student's name in the story.[3] The e-mail messages exchanged between Gonda and Baker were private, and not available in any publicly accessible portion of the Internet.[4]

Baker was arrested on the complaint and warrant on February 9, 1995, and detained overnight. The complaint and warrant is dated the same day. The following day, February 10, 1995, after holding a hearing a Magistrate Judge ordered Baker detained as a danger to the community. His detention was affirmed by a United States District Judge later that day. On March 8, 1995, this Court held a hearing on Baker's motion to be released on bond, and ordered that a psychological evaluation of Baker be performed. The psychological evaluation was received on March 10, 1995. The evaluation concluded that Baker did not pose a threat, and the Court ordered him released that day.[5]

On February 14, 1995 the government charged Baker with violating 18 U.S.C. ¤ 875(c) in a one count indictment based on unspecified communications transmitted in interstate and foreign commerce from December 2, 1994 through January 9, 1995. Presumably included in the communications was the story Baker posted. On March 15, 1995, the government charged Baker and Gonda in a superseding indictment with five counts of violating 18 U.S.C. ¤ 875(c). The story on which the initial complaint was partially based is not mentioned in the superseding indictment, which refers only to e-mail messages exchanged

between Gonda and Baker.[6] The government has filed a bill of particulars identifying who it perceives to be the objects of the allegedly threatening transmissions, as well as witness and exhibit lists.

Baker, who is named in all five of the superseding indictment's counts, has filed a motion seeking dismissal of all the counts of the superseding indictment. He contends that application of 18 U.S.C. ¤ 875(c) to the e-mail transmissions pushes the boundaries of the statute beyond the limits of the First Amendment. The government responds that the motion must be denied because the First Amendment does not protect "true threats," and because whether a specific communication constitutes a true threat is a question for the jury.

III. The Law

Eighteen U.S.C. ¤ 875(c) reads:

> Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

The government must allege and prove three elements to support a conviction under ¤ 875(c): "(1) a transmission in interstate [or foreign] commerce; (2) a communication containing a threat; and (3) the threat must be a threat to injure [or kidnap] the person of another." *United States v. DeAndino*, 958 F.2d 146, 148 (6th Cir.), *cert. denied*, 112 S. Ct. 2997 (1992). The Court of Appeals for the Sixth Circuit, like most others, has held that ¤ 875(c) requires only general intent. *Id.* at 149. *But see*, *United States v. Twine*, 853 F.2d 676 (9th Cir. 1988) (finding a specific intent requirement in ¤ 875(c)).[7] Because ¤ 875(c) is a general intent crime, intent must be proved by "objectively looking at the defendant's behavior in the totality of the circumstances," rather than by "probing the defendant's subjective state of mind." *DeAndino*, 958 F.2d at 149. The Sixth Circuit has also held that "a specific individual as a target of the threat need not be identified." *United States v. Cox*, 957 F.2d 264, 266 (6th Cir. 1992). Even so, the threat must be aimed as some discrete, identifiable group. *See id.* (involving threat to "hurt people" at a specific bank); *United States v. Lincoln*, 589 F.2d 379 (8th Cir. 1979) (involving letters threatening to kill judges of the Eighth Circuit, under 18 U.S.C. ¤ 876). The threat need not be communicated to the person or group identified as its target. *See United States v. Schroeder*, 902 F.2d 1469, 1470-71 (10th Cir.), *cert. denied*,, 498 U.S. 867 (1990) (affirming ¤ 875(c) conviction for a threat against people at a post office made to an Assistant United States Attorney); *United States v. Kosma*, 951 F.2d 549, 555 (3rd Cir. 1991) (listing cases in which threats against the President were made to third persons, under 18 U.S.C. ¤ 871).

Because prosecution under 18 U.S.C. ¤ 875(c) involves punishment of pure speech,[8] it necessarily implicates and is limited by the First Amendment. Although the Supreme Court has not addressed the constitutionally permissible scope of ¤ 875(c), it has considered a similar statute concerning threats against the President, 18 U.S.C. ¤ 871(a),[9] in *Watts v. United States*, 394 U.S. 705. In *Watts*, the Supreme Court recognized that:

> a statute such as this one, which makes criminal a form of pure speech, must be interpreted with the commands of the First Amendment clearly in mind. What is a threat must be distinguished from what is constitutionally protected speech.

Id. at 707. Under *Watts*, to pass constitutional muster the government must initially prove "a true 'threat.'" *Id.* Factors mentioned in *Watts* as bearing on whether a specific statement can be taken as a true threat include the context of the statement, including whether the statement has a political dimension; whether the statement was conditional; and the reaction of the listeners. *Id.*[10] *Watts* also makes clear that the question of whether a statement constitutes a true threat in light of the First Amendment is distinct from the question of the defendant's intent: "whatever the 'willfulness' requirement implies, the statute initially requires the Government to prove a true 'threat.'" *Id.*[11]

The distinction between the two questions of whether a statement is a "true threat" for the purposes of First Amendment limitation, and the intention of the statement's maker, is important but unfortunately often confused. The confusion results from too loose a use of the phrase "true threat."

The only extended discussion of the constitutional dimension of the "true threat" requirement with regard to ¤ 875(c) is found in *United States v. Kelner*, 534 F.2d 1020 (2d Cir.), *cert. denied*, 429 U.S. 1022 (1976). In *Kelner*, the Second Circuit drew on *Watts* to illuminate the constitutional limits of a prosecution under ¤ 875(c):

> The purpose and effect of the *Watts* constitutionally-limited definition of the term "threat" is to insure that only unequivocal, unconditional and specific expressions of intention immediately to inflict injury may be punished--only such threats, in short, as are of the same nature as those

> threats which are . . . "properly punished every day under statutes prohibiting extortion, blackmail and assault without consideration of First Amendment issues." *Watts*, 402 F.2d at 690.
>
> * * *
>
> So long as the threat on its face and in the circumstances in which it is made is so unequivocal, unconditional, immediate and specific as to the person threatened, as to convey a gravity of purpose and imminent prospect of execution, the statute may properly be applied. This clarification of the scope of 18 U.S.C. ¤ 875(c) is, we trust, consistent with a rational approach to First Amendment construction which provides for governmental authority in instances of inchoate conduct, where a communication has become "so interlocked with violent conduct as to constitute for all practical purposes part of the [proscribed] action itself."

Kelner, 534 F.2d at 1027 (quoting T. Emerson, The System of Freedom of Expression, 329 (1970)). *Cf. Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) ("the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.")

The government argues that the standard announced in *Kelner* is "far more stringent" than the governing standard in the Sixth Circuit. For the Sixth Circuit "true threat" standard, the government refers the Court to *United States v. Lincoln*, 462 F.2d 1368, *cert. denied*, 409 U.S. 952 (1972). In citing *Lincoln* for the "true threat" standard, the government confuses the constitutional "true threat" requirement with the statutory intent requirement. In relevant part, *Lincoln* reads:

> This Court therefore construes *the willfulness requirement of the statute* to require only that the defendant intentionally make a statement, written or oral, in a context or under such circumstances wherein a reasonable person would foresee that the statement would be interpreted by those to whom the maker communicates the statement as a serious expression of an intention to inflict bodily harm upon or take the life of the President, and that the statement not be the result of mistake, duress, or coercion. The statute does not require that the defendant actually intend to carry out the threat.

Lincoln, 462 F.2d at 1368 (quoting and adopting standard from *Roy v. United States*, 416 F.2d 874, 877-78 (9th Cir. 1969)) (emphasis added). *Lincoln* addresses the statute's intent requirement, and adopts the Ninth Circuit's formulation of the intent required.[12] It does not speak to the constitutional "true threat" requirement imposed by the First Amendment and elucidated in *Watts* and *Kelner*. *United States v. Glover*, 846 F.2d 339, 343-44 (6th Cir.), *cert. denied*, 488 U.S. 982 (1988) and *United States v. Vincent*, 681 F.2d 462, 464 (6th Cir. 1982), also cited by the government, quote the same language from *Roy* and also address the statutory intent requirement rather than the constitutional limits of the statute. None of these cases indicate that a different constitutional standard for prosecution under ¤ 875(c) applies in the Sixth Circuit than in the Second Circuit.[13]

The confusion between the two requirements is understandable, because the phrase "true threat" has been used in the context of both requirements. Both the Ninth and Seventh Circuits have stated that the government must meet the *Roy* general intent standard in order to make out a "true threat." *Melugin v. Hames*, 38 F.3d 1478, 1484 (9th Cir. 1994) (under Alaska statute AS 11.56.510(a)(1)); *United States v. Khorrami*, 895 F.2d 1186, 1193 (7th Cir.), *cert. denied*, 498 U.S. 986 (1990). That the phrase "true threat" has been used to describe both the statutory intent requirement and the constitutional "unconditional, unequivocal, immediate and specific" requirement does not imply that the two requirements are identical, or that any statement which meets the intent requirement may be prosecuted under ¤ 875(c) without running afoul of the First Amendment. Typically, in the cases focussing on the intent requirement, there is no dispute that the statement satisfies the constitutional standard, and the defendant seeks dismissal or reversal of his conviction on the ground that he or she lacked the requisite intent. *See*, *e.g.*, *United States v. Lincoln*, 462 F.2d at 1369 ("[a]pellant contends that the statute is violated only when a threat is uttered with a willful intent to carry it out."); *United States v. Hoffman*, 806 F.2d 703, 712 (7th Cir. 1986) (concluding that "it was reasonable for the jury to conclude that Hoffman intended the letter as a serious expression of his intent to harm the President.") (quoted in *Khorrami*, 895 F.2d 1186).[14]

Kelner's standard for a prosecution under 18 U.S.C. ¤ 875(c) is not only constitutionally required, but also is consistent with the statute's legislative history. The law which was eventually codified as 18 U.S.C. ¤ 875(c) was first passed in 1932, Pub. L. No. 72-274 (1932), and criminalized use of the mail to transmit a threat to injure or kidnap any person (or to injure a person's property or reputation), or to accuse a person of a crime or demand ransom for a kidnapped person. *Id*. The communication had to be sent "with intent to extort . . . money or any thing of value" to fall under the act. *Id*. A motivating factor for passage of the 1932 act was the kidnapping of Charles Lindbergh's son, and the concomitant use of the mail to convey the kidnappers' threats and demands. H.R. Rep. No. 602, 72d Congress, 1st Sess. (1932).

The act was addressed to the constitutionally unproblematic case, like the Lindbergh case, identified in *Kelner*: "where a communication has become 'so interlocked with violent conduct as to constitute for all practical purposes part of the [proscribed] action itself.'" *Kelner*, 534 F.2d at 1027. The act was modified in 1934, Pub. L. No. 73-231 (1934), as increasingly sophisticated criminals had taken to using means other than the mail, such as the telephone and telegraph, to transmit their threats. S. Rep. No. 1456, 73d Congress, 2d Sess. (1934). As modified, it applied to threats transmitted "by any means whatsoever," but still required extortionate intent. Pub. L. No. 73-231 (1934). In 1939 the act, Pub. L. No. 76-76 (1939), was expanded to apply to threats to kidnap or injure that were not made with extortionate intent. *Id*. The act's expansion was prompted by the recognition that many threats "of a very serious and socially harmful nature" were not covered by the existing law because "the sender of the threat did not intend to extort money or other thing of value for himself." H.R. Rep. No. 102, 76th Congress, 1st Sess. (1939). An example of such a threat mentioned in the in the Report was one directed to a governor, threatening to blow up the governor's home if certain defendants in a criminal case were not released. As modified, while an "extortionate" intent was no longer required, the act was still intended to address threats aimed at accomplishing some coercive purpose, such as the release of the defendants in the given example. The modified statute still targets threats which, like the example, are unlikely to offend the constitutional standard articulated in *Kelner*.

Threats aimed at achieving some coercive end remain the typical subject of more contemporary cases. In *Cox*, for instance, the defendant's truck was repossessed while it contained items of his personal property. The defendant telephoned the bank that had had the truck repossessed and stated "I tell you what, you all better have my personal items to me by five o'clock today or it[']s going to be a lot of hurt people there." *Cox*, 957 F.2d at 265. The threat was designed to effect the return of the defendant's property, it targeted the people at the bank, and it was found not to be conditional (in part because his property could not have been returned by the five o'clock deadline). It falls within *Kelner*'s requirement of a threat that is "so unequivocal, unconditional, immediate and specific as to the person threatened, as to convey a gravity of purpose and imminent prospect of execution." 534 F.2d at 1027.

Similarly, in *Schroeder*, the defendant had sued the government for denial of employment preference under a veterans benefit program. 902 F.2d at 1470. After losing his civil suits, the defendant called an Assistant United States Attorney and threatened to shoot people at a post office if he did not obtain satisfaction from the government; he stated that "the government either gives [him] money or people would get hurt." *Id*. *Schroeder* involves an explicitly extortionate threat aimed at people in post offices. Although the case appears to strain the constitutional standard, particularly with regard to the requirement of immediacy, the defendant did not raise a constitutional challenge on appeal.

While coercive or extortionate threats are paradigmatic subjects of a prosecution under 18 U.S.C. ¤ 875(c), a threat which is neither coercive nor extortionate may still satisfy the constitutional test from *Kelner*; indeed, *Kelner* itself involved a non-coercive threat to assassinate the PLO leader Yasser Arafat. *Kelner*, 534 F.2d at 1025. *See also*, *DeAndino*, 958 F.2d at 146 (regarding threat that defendant was going to "blow [the victim's] brains out," and the victim was "going to die.") Nevertheless, a coercive or extortionate threat is particularly likely to be a constitutionally prosecutable "true threat" because it is particularly likely to be intimately bound up with proscribed activity.

Another important factor in analyzing a threat under 18 U.S.C. ¤ 875(c) is the recipient of the communication in question. As the Sixth Circuit stated in *Lincoln* (in the context of ¤ 871(a)), the statutory general intent element requires that "a reasonable person would foresee that the statement would be interpreted *by those to whom the maker communicates the statement* as a serious expression of an intent to inflict bodily harm" or kidnap a person. 462 F.2d at 1368. Thus in *Cox*, the Sixth Circuit looked to the reaction of the recipient of the defendant's telephone call, as well as that of the person to whom the defendant asked to speak.[15] *Cox*, 957 F.2d at 266. In *Schroeder*, the appropriate focus in considering the defendant's statements is how they would be interpreted by the Assistant United States Attorney who heard them, and by those to whom we could foreseeably relay them. A statement which would not be interpreted by any foreseeable recipient as expressing a serious intention to injure or kidnap simply is not a threat under the statute. While it is not necessary that the statement prosecuted under 18 U.S.C. ¤ 875(c) be communicated to the would-be target of the alleged threat, the statement must be evaluated in light of foreseeable recipients of the communication.

Evaluating a statement charged under 18 U.S.C. ¤ 875(c) in light of its foreseeable recipients is consistent with the aims of the statute and the First Amendment. In the case of a coercive or extortionate threat, the maker of the statement obviously cannot achieve his or her end if the recipient of the statement does not take it as expressing a serious intention to carry out the threatened acts. If the coercive or extortionate threat is likely to be taken seriously by its recipient, then the threat is "so interlocked with violent conduct as to constitute for all practical purposes part of the [proscribed] action itself." *Kelner*, 534 F.2d at 1027. A communication containing an alleged non-coercive threat may be regulated consonant with the First Amendment, under the analysis in *R.A.V. v. City of St. Paul*, ___ U.S. ___, ___, 120 L.Ed.2d 305, 321 (1992), in order to "protect[] individuals from the fear of violence, from the disruption that fear engenders, and from the possibility that the threatened violence will occur." If the alleged threat would not be interpreted by its foreseeable recipients as a serious

expression of an intention to do the "threatened" acts, it does not implicate fear of violence or the disruption that fear engenders, and does not suggest a real possibility that the "threatened" violence will occur. The statement thus would not be a "true threat" for the purposes of the First Amendment.

Whether or not a prosecution under ¤ 875(c) encroaches on constitutionally protected speech is a question appropriately decided by the Court as a threshold matter. In the context of the Smith Act, 18 U.S.C. ¤ 2381 *et seq*., which makes it a crime knowingly or willfully to advocate the overthrow or destruction of the United States government by force or violence, the Supreme Court has held that "[w]hen facts are found that establish the violation of a statute, the protection against conviction afforded by the First Amendment is a matter of law" requiring a judicial determination. *Dennis v. United States*, 341 U.S. 494, 513 (1951) (construing Act as codified at 18 U.S.C. (1946 ed.) ¤ 11, 54 Stat. 671). In the context of ¤ 875(c), the Second Circuit has recognized that "[m]ost cases are within a broad expanse of varying fact patterns which may not be resolved as a matter of law, but should be left to a jury," but has said that where the factual proof of a "'true' threat" is "insufficient as a matter of law," the indictment is properly dismissed before reaching the jury. *United States v. Carrier*, 672 F.2d 300, 306 (2d Cir.), *cert. denied*, 457 U.S. 1139 (1982). Although the government argues that "whether a statement is a true threat is to be decided by the trier of fact," it recognizes that where "the language set forth . . . is so facially insufficient that it cannot possibly amount to a true threat," the Court may properly dismiss the indictment. *Id.*; *accord Kosma*, 951 F.2d at 555; *United States v. Gilbert*, 884 F.2d 454, 458 (9th Cir. 1989), *cert. denied*, 493 U.S. 1082 (1990); *United States v. Howell*, 719 F.2d 1258, 1260 (5th Cir. 1983), *cert. denied*, 467 U.S. 1228 (1984); *Lincoln*, 589 F.2d at 382. Whether the language set forth in the superseding indictment could possibly constitute a "true threat" must be determined in accord with *Kelner*'s articulation of the constitutional requirement of a

> threat which on its face and in the circumstances in which it is made is so unequivocal, unconditional, immediate and specific as to the person threatened, as to convey a gravity of purpose and imminent prospect of execution.

Kelner, 534 F.2d at 1027. Whether or not Baker actually intended to carry out the actions described in the communications is irrelevant to the constitutional inquiry.

IV. The Communications

The government characterizes the e-mail dialogue between Gonda and Baker in December, 1994 as reflecting "the evolution of their activity from shared fantasies to a firm plan of action." The government's characterization of the ongoing dialogue suggests that at least some of the counts in the superseding indictment should be dismissed; messages constituting "shared fantasies" fall short of the *Kelner* standard of an unequivocal, unconditional, immediate and specific threat conveying an imminent prospect of execution and therefore are not "true threats" unprotected by the First Amendment.

As the Court construes the law as discussed above, the constitutional standard enunciated in *Kelner* requires, at the very least, that a statement charged under ¤ 875(c) contain some language construable as a serious expression of an intent imminently to carry out some injurious act. The language of the statement must be considered as it would be interpreted by the foreseeable recipients of the communication containing it. Statements expressing musings, considerations of what it would be like to kidnap or injure someone, or desires to kidnap or injure someone, however unsavory, are not constitutionally actionable under ¤ 875(c) absent some expression of an intent to commit the injury or kidnapping.[16] In addition, while the statement need not identify a specific individual as its target, it must be sufficiently specific as to its potential target or targets to render the statement more than hypothetical.

Before addressing the specific language quoted in the indictment, several observations pertain to all of the government's charges. First, all of the language for which Baker is charged was contained in private e-mail messages he sent to Gonda. The messages were not available in any publicly accessible part of the Internet, and there is no allegation that they were ever distributed in any format, electronic or hardcopy, to anyone other than Gonda. Nothing in these private messages suggests that they would be further distributed. It is only as a result of this prosecution and the ensuing publicity that the content of the messages has been publicly aired.

The focus of the inquiry here, therefore, is how a reasonable person would expect Gonda to interpret the e-mail messages. Gonda's identity is entirely unknown; "he" could be a ten year old girl, an eighty year old man, or a committee in a retirement community playing the role of Gonda gathered around a computer.[17] All that is known about Gonda is that he used a computer account based in Ontario, Canada, and that he apparently enjoyed exchanging with Baker what he referred to in an e-mail message dated January 3, 1995, as "REAL sex talk" concerning violence against women and girls. The language referred to by the government clearly does not constitute threats of a coercive or extortionate nature. It would be patently unreasonable after reading his messages to think that Baker's communications caused their only foreseeable recipient, Gonda, to fear violence, or caused him any disruption due to fear of violence. Of the grounds for prosecution of threats identified in *R.A.V.*,

the only one that could apply here is protection from the possibility that threatened violence will occur. ___ U.S. at ___, 120 L.Ed.2d at 321.

The government characterizes the communications between Gonda and Baker as evolving into "a firm plan of action." Section 875(c), though, does not address planning crimes, per se, but transmitting threats to injure or kidnap. At oral argument, the government agreed the exchange between Gonda and Baker could be characterized as an exchange between coconspirators. In order to prove the existence of a conspiracy, generally, the government must prove an agreement between two or more people to act together in committing an offense, and also an overt act in furtherance of the conspiracy. *E.g.*, *United States v. Reifsteck*, 841 F.2d 701, 704 (6th Cir. 1988); 18 U.S.C. ¤ 371; Sixth Circuit Pattern Criminal Jury Instructions 3.01A, 3.04. The charges here could not support a conspiracy prosecution because no overt act is alleged. The only actions involved in this prosecution are speech--"the outward expression of what a person thinks in his mind." *Vance v. Judas Priest, et al.*, 1990 WL 130920, *28 (Nev. Dist. Ct. 1990). In an e-mail exchange not quoted in the superseding indictment,[18] Baker and Gonda discuss sharing their thoughts, a classically protected activity. Baker had said to Gonda, in part: "I'd love to meet with you. There's no one else I can share my thoughts with." On November 29, 1994, Gonda responded in part: "I would really love to meet with you. I find that I am going insane trying to keep all these thoughts to myself. . . maybe we could even try to pick up some chicks and share our thoughts with them. . . what do you think?"

Even if Gonda and Baker were conspiring, it does not follow that they are guilty of transmitting a threat to injure or kidnap under 18 U.S.C. ¤ 875(c). Section 875(c) is not simply a conspiracy statute minus the overt act requirement. In order to be constitutionally sanctionable, the statements Baker made must meet *Kelner*'s "unequivocal, unconditional, immediate, and specific" standard. As Justice Brandeis wrote:

> Fear of serious injury cannot alone justify suppression of free speech. . . To justify suppression of free speech there must be reasonable ground to fear that serious evil will result if free speech is practiced. There must be reasonable ground to believe that the danger apprehended is imminent.

Whitney v. California, 274 U.S. 357, 376 (1927) (Brandeis, J., concurring).[19]

A.

Count I charges Baker and Gonda with transmitting a threat to injure, and quotes from three e-mail messages. In the first message quoted, dated December 1, 1994, Baker responds to a message he had received from Gonda:

> I highly agree with the type of woman you like to hurt. You seem to have the same tastes I have. When you come down, this'll be fun!
>
> Also, I've been thinking. I want to do it to a really young girl first. !3 or 14.[20] There innocence makes them so much more fun --- and they'll be easier to control. What do you think? I haven't read your entire mail yet. I've saved it to read later, in private. I'll try to write another short phantasy and send it. If not tomorrow, maybe by Monday. No promises.

On December 2, Gonda responded:

> I would love to do a 13 or 14 year old. I think you are right...not only their innocence but their young bodies would really be fun to hurt. As far as being easier to control...you may be right, however you can control any bitch with rope and a gag...once tey are tieed up and struggling we could do anything we want to them...to any girl. The trick is to be very careful in planning. I will keep my eye out for young girls, and relish the fantasy...BTW[21] how about your neighbour at home, youm may get a chance to see her...?...?

The same day, Baker responded:

> True. But young girls still turn me on more. Likely to be nice and tight. Oh.they'd scream nicely too!
>
> Yeah. I didn't see her last time I was home. She might have moved. But she'd be a great catch. She's real pretty. with nice long legs. and a great girly face ... I'd love to make her cry ...

The bill of particulars identifies the targets of these statements as:

> 13 and 14-year old girls who reside in Defendant Jake Baker's neighborhood in Ann Arbor, Michigan, and teen-age girls who reside in Defendant Jake Baker's neighborhood in Boardman, Ohio.

This Count falls short of the constitutional "true threat" requirement. As an initial matter, it does not refer to a sufficiently specific class of targets. The more limited class identified in the bill of particulars is not apparent from the face of the communications. Nothing in the exchange quoted in Count I implicitly or explicitly refers to 13 or 14 year old girls *in Ann Arbor*, nothing in the exchange identifies Boardman, Ohio (Baker's actual home) as the "home" referred to, and nothing in the exchange allows one to determine that the neighbor discussed is a teen-age girl. In reality, the only class of people to whom the messages can be taken to refer is 13 or 14 year old girls, anywhere. This class is too indeterminate to satisfy *Kelner*'s requirement of specificity as to the person threatened, even under the liberal interpretation given the requirement by some courts. *Cf. Schroeder*, 902 F.2d at 1470 (targeting people at an unidentified post office).

As to the content of the messages, Baker's discussing his "tastes" in the first paragraph of his December 1 message does not involve any identifiable threatened action. In the second paragraph of the December 1 message, he expresses a desire "to do it to" a 13 or 14 year old girl. Even assuming that more context would clarify the phrase "to do it to," the second paragraph also fails to mention an intention to do anything. Rather, it seeks Gonda's reaction to Baker's desire, asking: "What do you think?" Discussion of desires, alone, is not tantamount to threatening to act on those desires. Absent such a threat to act, a statement is protected by the First Amendment.

As to Baker's message of December 2, the first paragraph again discusses a predilection toward "young girls," and what it would be like, presumably, "to do it to" "young girls." It does not mention any intention to act in accordance with the expressed predilection. The second paragraph responds to Gonda's question about a neighbor "at home." It says "she'd be a great catch," but expresses no intention to "catch" her, and indicates a desire to "make her cry," but, again, expresses no intention to take any action in accordance with that desire. It is not constitutionally permissible under *Kelner* to infer an intention to act on a desire from a simple expression of the desire. The intention (whether or not actually held) must itself be expressed in the statement. Count I fails to meet this standard, and must be dismissed.

B.

Counts II and III are based on the same statement made by Baker in an e-mail message dated December 9, 1994, and charge Baker with making a threat to kidnap and a threat to injure, respectively. The statement for which Baker is charged in the two counts reads:

> I just picked up Bllod Lust and have started to read it. I'll look for "Final Truth" tomorrow (payday). One of the things I've started doing is going back and re-reading earlier messages of yours. Each time I do. they turn me on more and more. I can't wait to see you in person. I've been trying to think of secluded spots. but my knowledge of Ann Arbor is mostly limited to the campus. I don't want any blood in my room, though I have come upon an excellent method to abduct a bitch ---
>
> As I said before, my room is right across from the girl's bathroom. Wiat until late at night. grab her when she goes to unlock the dorr. Knock her unconscious. and put her into one of those portable lockers (forget the word for it). or even a duffle bag. Then hurry her out to the car and take her away ... What do you think?

The bill of particulars identifies the target of the statement as: "Female college students who lived in Defendant Jake Baker's dormitory at the University of Michigan in Ann Arbor, Michigan." Apart from concerns about equating Baker's on-line persona with his real person, the class of would-be targets here is identified with sufficient specificity.

Presumably, the government offers this statement as a threat to carry out the "method to abduct" it describes. Under *Kelner*, discussion of a method of kidnapping or injuring a person is not punishable unless the statement includes an unequivocal and specific expression of intention immediately to carry out the actions discussed. Baker's e-mail message cannot reasonably be read as satisfying this standard. As in Count I, the language with which Baker is charged here lacks any expression of an intention to act, and concludes with a request for Gonda's reaction: "What do you think?" Discussing the commission of a crime is not tantamount to declaring an intention to commit the crime. To find an expression of unequivocal intention in this language would require the drawing of an inference not grounded in any specific language of the statement and would exceed the bounds of the First Amendment. Counts II and III must be dismissed.

C.

Count IV charges Baker and Gonda with transmitting a threat to injure. The Count is based on a message from Gonda to Baker, and Baker's response. Both e-mail messages are dated December 10, 1994. Gonda wrote:

> Hi Jake. I have been out tonight and I can tell you that I am thinking more and more about 'doing' a girl. I can picture it so well...and I can think of no better use for their flesh. I HAVE to make a bitch suffer!
>
> As far as the Teale-homolka killings, well I can think of no tastier crimes...BTW have you seen any pictures of the girls? You have to see these cunts! They must have been so much fun...please let me know any details that I cannot get here. I would love to see what you think about it....
>
> As far as the asian bitch story, there is only one possible ending....

Baker responded:

> Are tastes are so similar. it scares me :-) When I lay down at night. all I think of before I sleep is how I'd torture a bitch I get my hands on. I have some pretty vivid near dreams too. I wish I could remember them when I get up.

The bill of particulars identifies the target of these statements as:

> Women who were the subject of Defendant Jake Baker's E-mail transmissions and Internet postings, including -- but not limited to -- Jane Doe, whose true name is known to Defendant Jake Baker and this Honorable Court.

This Count presents the weakest of all the government's charges against Baker. While the government identifies the class of targets here as women Baker discussed on the Internet, there is nothing in the language quoted here to so limit the class. In addition, since Baker's e-mail often refers simply to "a girl," a class composed of women Baker discussed in his e-mail and stories essentially is a class composed of any woman or girl about whom Baker has ever thought. Such a class is obviously not sufficiently specific.

With regard to the content of Baker's communication, Baker's statement here consists only of an expression of his thoughts before sleeping and of "near dreams" he cannot remember upon waking. To infer an intention to act upon the thoughts and dreams from this language would stray far beyond the bounds of the First Amendment, and would amount to punishing Baker for his thoughts and desires. Count IV must be dismissed.

D.

Count V charges Baker and Gonda with transmitting a threat to injure. It is based on an exchange between Gonda and Baker on December 11-12, 1994. On December 11, Gonda wrote to Baker:

> It's always a pleasure hearing back from you...I had a great orgasm today thinking of how you and I would torture this very very petite and cute south american girl in one of my classes...BTW speaking of torture, I have got this great full length picture of the Mahaffy girl Paul Bernardo killed, she is wearing this short skirt!

The same day, Baker responded:

> Just thinking about it anymore doesn't do the trick ... I need TO DO IT.

The next day, Gonda wrote:

> My feelings exactly! We have to get together...I will give you more details as soon as I find out my situation...

Baker responded:

> Alrighty then. If not next week. or in January. then definatly sometime in the Summer. Pickings are better then too. Although it's more crowded.

The bill of particulars identifies the target of these statements, as in Count IV, as:

> Women who were the subject of Defendant Jake Baker's E-mail transmissions and Internet postings, including -- but not limited to -- Jane Doe, whose true name is known to Defendant Jake Baker and this Honorable Court.

This Count, too, fails to meet *Kelner*'s constitutional "true threat" standard. The class of potential targets, as discussed with regard to Count IV, is far too vague. As to the content of the communications, Baker indicates his

"need TO DO IT." Like his earlier statements, this language indicates a desire to do something. While use of the word "need" indicates a strong desire, it still falls short "unequivocal, unconditional and specific expression of intention immediately to inflict injury," *Kelner*, 534 F.2d at 1027; "needs" go unmet everyday. Baker next indicates, at most, an intention to meet Gonda at some indefinite point in the future--in the next week, month, or several months later. This statement does not express an unequivocal intention immediately to do anything. Also, nothing in the language on which the Count is based indicates any intention to commit specific acts if Baker and Gonda ever were to meet. Like the preceding four Counts, Count V fails to state a charge under ¤ 875(c) that can survive a First Amendment challenge, and must be dismissed. This prosecution presents the rare case in which, in the government's words, "the language set forth . . . is so facially insufficient that it cannot possibly amount to a true threat."

V. Coda

This case in its initial stage generated a good deal of public interest.[22] Now that the case will be concluded by an order rather than by a jury verdict, it is important to assure the public that such a conclusion is not by fiat. In *United States v. Carrier*, 672 F.2d 300, 306 (2d Cir.), *cert. denied*, 457 U.S. 1139 (1982), while the Second Circuit said "that whether words used are a true threat is generally best left to the triers of fact," it went on to say "[o]nly where the factual proof is insufficient as a matter of law should the indictment be dismissed." This is such a case. The communications which form the basis of the superseding indictment, the many preceding and subsequent communications, the names of the witnesses and the general nature of their testimony, and the exhibits are all in the record. All of this evidence, viewed in the light most favorable to the prosecution, leads to one inevitable conclusion: based on the applicable rules of law there is no case for a jury because the factual proof is insufficient as a matter of law. The government's enthusiastic beginning petered out to a salvage effort once it recognized that the communication which so much alarmed the University of Michigan officials was only a rather savage and tasteless piece of fiction. Why the government became involved in the matter is not really explained in the record.[23]

Baker is being prosecuted under 18 U.S.C. ¤ 875(c) for his use of words, implicating fundamental First Amendment concerns. Baker's words were transmitted by means of the Internet, a relatively new communications medium that is itself currently the subject of much media attention. The Internet makes it possible with unprecedented ease to achieve world-wide distribution of material, like Baker's story, posted to its public areas. When used in such a fashion, the Internet may be likened to a newspaper with unlimited distribution and no locatable printing press--and with no supervising editorial control. But Baker's e-mail messages, on which the superseding indictment is based, were not publicly published but privately sent to Gonda. While new technology such as the Internet may complicate analysis and may sometimes require new or modified laws,[24] it does not in this instance qualitatively change the analysis under the statute or under the First Amendment. Whatever Baker's faults, and he is to be faulted, he did not violate 18 U.S.C. ¤ 875(c). The case would have been better handled as a disciplinary matter, as the University of Victoria proceeded in a similar situation,[25] despite whatever difficulties inhere in such a course.[26] What the Court said at the conclusion of oral argument bears repeating: "[T]he Court is very skeptical, and about the best thing the government's got going for it at this moment is the sincerity of purpose exhibited by [the Assistant United States Attorneys prosecuting the case]. I am not sure that sincerity of purpose is either synonymous with a good case under the law, or even the exercise of good judgment."

AVERN COHN

UNITED STATES DISTRICT JUDGE

DATED: June 21, 1995
Detroit, Michigan

Chiamata in giudizio del caso Woodside

UNITED STATES DISTRICT COURT EASTERN DISTRICT OF NEW YORK

JAYNE A. HITCHCOCK, Plaintiff,

-against-

WOODSIDE LITERARY AGENCY, JAMES LEONARD, SUSAN DAY, JOHN LAWRENCE, RICHARD BELL, URSULA SPRACHMANN, and JOHN DOE #1 through JOHN DOE #10, the preceding ten names being fictitious, the persons or parties intended being the persons doing business as Woodside Literary Agency and/or James Leonard, Susan Day, John Lawrence, Richard Bell, or Ursula Sprachmann, and RICHARD ROE #1 through RICHARD ROE #10, the last preceding ten names being fictitious, the persons or parties intended being the persons acting in concert with the named defendants and/or defendants John Doe #1 through John Doe #10 in connection with the matters described in the complaint,

Defendants,

Case No. 97 Civ. 0166 (Gershon)

COMPLAINT

Plaintiff, by her attorney, John A. Young, for her complaint herein, alleges: Jurisdiction of this Court

1. This Court has jurisdiction over this action by virtue of 18 U.S.C. 1964(c) and 28 U.S.C. 1331, 1332.

2. Identification and citizenship of plaintiff: Plaintiff, Jayne A. Hitchcock, resides in, and is a citizen of, the State of Maryland.

3. Identification and citizenship of defendants:

1. Named defendants:

1. Upon information and belief, defendant Woodside Literary Agency ("Woodside"), is an enterprise owned and operated by defendants, James Leonard, Susan Day, John Lawrence, Richard Bell, Ursula Sprachmann, and John Doe #1 through John Doe #10.

2. Upon information and belief, defendant Woodside has not been officially organized under the laws of the any state of the United States of America.

3. Upon information and belief, defendant Woodside has its principal place of business in the state of New York, within the Eastern District of New York.

4. Upon information and belief, each of the named defendants is a citizen of the State of New York or of the State of Florida.

 Defendants John Doe #1 through John Doe #10 (the "Doe defendants"):

1. Upon information and belief, each of the Doe defendants is a person not actually named "James Leonard", "Susan Day", "John Lawrence", "Richard Bell", or "Ursula Sprachmann" who does business under one or more of such names and/or the name "Woodside Literary Agency".

2. Upon information and belief, each of the Doe defendants is a citizen of foreign state or of a state other than the State of Maryland.

3. Upon ascertaining the true identities of the Doe defendants, plaintiff intends to file an amended complaint which will identify them more specifically.

 Defendants Richard Roe #1 through Richard Roe #10 (the "Roe defendants"):

1. Upon information and belief, each of the Roe defendants is a person not actually named "James Leonard", "Susan Day", "John Lawrence", "Richard Bell", or "Ursula Sprachmann" who conspired, cooperated, assisted, aided or abetted one or more of the named defendants or Doe defendants in committing the acts hereinafter complained of.

2. Upon information and belief, each of the Roe defendants is a citizen of foreign state or of a state other than the State of Maryland.

3. Upon ascertaining the true identities of the Roe defendants, plaintiff intends to file an amended complaint which will identify them more specifically.

 The matter in controversy exceeds, exclusive of interest and costs, the sum of fifty thousand dollars.
 Upon information and belief, Woodside is an enterprise within the definition contained in the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. Secs. 1961-68, 1961(4) in connection with which the named defendants other than Woodside, together with the Doe defendants and with the assistance of the Roe defendants, conduct activities prohibited by 18 U.S.C. Sec. 1962. Background
 Plaintiff is a professional author and a Teaching Assistant at the University of Maryland.
 Plaintiff makes extensive use of electronic mail ("E-mail") and other internet services for her business and professional activities. Plaintiff also uses internet services including E-mail for personal purposes.
 Plaintiff frequently reads and posts articles to an internet news group called "misc.writing" which is followed by many authors and would-be authors.
 Defendants have posted or caused to be posted messages to the "misc.writing" news group and other internet news groups numerous advertisements on behalf of "Woodside Literary Agency" soliciting writing samples from published and unpublished authors.
 The posting of advertisements to internet news groups (other than a few groups which exist specifically for that purpose) is generally considered an abuse of the internet and of the readers of the news groups.
 The posting of the same, or virtually the same, message to many news groups or many times, a practice generally known as "spamming", is also generally considered an abuse of the internet and of the readers of the news groups.
 Literary agents are a recognized and respected part of the publishing industry. The regular course of business for a normal literary agent is to represent the author in business discussions and negotiations with potential publishers of the author's work in exchange for a fee which is earned upon the sale of a work and paid out of a modest portion of the proceeds of such sale.
 Notwithstanding Woodside's inappropriate posting of its advertisement on the "misc.writing" newsgroup, plaintiff responded to it. Woodside replied with a letter praising the sample of her work and suggesting that she send it the full manuscript together with $75 as a "reading and market evaluation fee".
 Wanting to be sure that said reply was not an isolated exception, plaintiff responded again to Woodside's advertisement, this time using her maiden name. Woodside's reply was virtually identical, except that it asked for a $150 "reading and market evaluation fee", and stated:

> The agent assigned to your submission is interested and would like to review the entire manuscript, re: When Will I See You Again. Please make a check out to Mr. John Lawrence (the agent reviewing your work) for $150.00. This reading and market evaluation fee is refundable upon the sale of your work and bank clearance of publisher's advance.
>
> "Please be advised that less than 5% of the authors contacting us are lucky enough to catch our interest. Obviously, Mr. Lawrence thinks you've got something good.
>
> "Kindly send the material to our NY main office by August 5th: (I advise you to Fed-X it on August 2nd so Mr. Lawrence gets it on the 3rd). From August 7th until the end of August he will be at the Florida branch. You may send your manuscript there anytime after August 7th-not before.
>
> "[signed]
> Senior Editor
> Dr. Richard Bell"

 From this, plaintiff concluded that Woodside was operated in a manner substantially different from that of a normal and legitimate literary agency.
 Upon information and belief, Woodside typically responds to a potential client's submission of a writing sample with a letter lauding the quality of the writing and requesting a "reading fee" of $150.00.

 Upon information and belief, Woodside is in the business of collecting "reading fees" and not in the business of representing authors in business discussions and negotiations with potential publishers.
 After learning the manner in which Woodside did business, plaintiff posted articles in response to Woodside's advertisements in internet news groups, in which articles she advised would-be authors of the facts that the normal and legitimate literary agencies did not charge "reading fees" or other fees in advance of making a sale; but that Woodside did so. She also objected to Woodside's spamming of newsgroups with advertisements and voiced her opinion that Woodside was a scam and not a legitimate literary agency.
 Plaintiff also reported the activities of Woodside to the Attorney General of the State of New York, and, upon information and belief, the Bureau of Consumer Frauds and Protection, of the New York State Department of Law, is conducting an investigation of Woodside as a result of that report.
 Thereafter, defendants committed the acts complained of herein. Plaintiff's Claim for Relief
 The named defendants and the Doe defendants have published or caused to be published numerous messages on internet news groups falsely accusing Jayne Hitchcock of being a "bored housewife" who was attacking Woodside because her writings were "PORN" which had been rejected.
 The named defendants and the Doe defendants have threatened to have Jayne Hitchcock blacklisted by publishers.
 The named defendants and the Doe defendants have harassed plaintiff and interfered with her ability to conduct business and personal communications by way of E-mail or other internet services or by telephone. The means of such harassment have included

1. Flooding plaintiff's E-mail accounts with hundreds of meaningless or abusive messages, many of which have been very lengthy, a practice known as "mail- bombing";

2. Posting messages in various internet news groups calculated to inflame most readers of those news groups ("flame-bait") and forging the origination information on those messages to make it appear that they were posted by Jayne Hitchcock, thereby inducing inflamed readers to send her E-mail complaints; and

3. Posting the messages described in the following paragraph of this complaint.

 The named defendants and the Doe defendants have placed Jayne Hitchcock in imminent danger of sexual assault, of other bodily harm, and of her very life, by posting to many internet news groups devoted to the topics of sex, and particularly of deviant sex, messages forged to appear to have originated from her such as the following

> "Female International Author, no limits to imagination and fantasies, prefers group macho/sadistic interaction, including lovebites and indiscriminate scratches. Invites you to write or call to exchange exciting phantasies with her which will be the topic of her next book. No fee or hidden expenses for talented partici pants. Contact me at misc.writing or stop by my house at [plaintiff's actual home address]. Will take your calls day or night at [plaintiff's actual home telephone number]. I promise you everything."

The named defendants and the Doe defendants have also attempted to interfere with plaintiff's business affairs by mail-bombing the University of Maryland and her own literary agent and by sending E-mail to them, forged to appear as though such E-mail had originated with her, and written in a manner calculated to disrupt her relationship with each of those institutions.

 Upon information and belief, some of the Roe defendants conspired, cooperated, assisted, aided or abetted one or more of the named defendants or Doe defendants in doing each of the acts described in paragraphs numbered "21" through "25" of this Complaint, and each of the Roe defendants conspired, cooperated, assisted, aided or abetted one or more of the named defendants or Doe defendants in doing some of such acts.
 Upon information and belief, each of the acts complained of above was done by the named defendants and the Doe defendants wilfully, wantonly and maliciously and with the specific intent to injure plaintiff
 Upon information and belief, each of the acts complained of above was done by the Roe defendants either wilfully, wantonly and maliciously and with the specific intent to injure plaintiff or with reckless disregard of their foreseeable consequences to plaintiff.
 As a result of the foregoing, plaintiff has suffered extreme emotional distress and has been substantially injured in her business and property.

WHEREFORE, plaintiff demands judgment against defendants, jointly and severally, awarding plaintiff:

1. Injunctive relief prohibiting defendants from any further conduct which would tend to harass plaintiff;

2. Threefold the compensatory damages determined by the trier of fact herein;

3. Punitive damages of $10,000,000 or in such other amount as may be determined by the trier of fact herein;
4. Her costs and disbursements herein, including a reasonable attorney's fee; and
5. Such other and further relief as this Court may deem just and proper in the premises.

Dated: New York, New York
January 13, 1997
John A. Young
EDNY attorney bar code JY1748
Attorney for plaintiff
P.O. Box 4695
New York, NY 10185-4695 [22 Wyckoff Street Brooklyn, NY 11201 (718) 875-0337]

Sentenza di Abdus-Salaam sul caso Woodside

Department of Law
120 Broadway
New York, NY 10271

Department of Law
The State Capitol
Albany, NY 12224

For More Information: (518) 473-5525

For Immediate Release
February 17, 1999

JUDGMENT OBTAINED AGAINST PHONY ON-LINE LITERARY AGENCY

Group of Writers Helps Expose Internet Publishing Scam

Attorney General Eliot Spitzer today announced a judgment against an Internet publishing company that lured aspiring writers into paying hundreds of dollars to get their work published, only to find out that the offer itself was a work of fiction.

The Woodside Literary Agency of Queens has been ordered to stop its Internet publishing scheme, provide restitution to consumers, pay penalties and costs to the state and post a $100,000 bond to protect consumers in future business dealings.

"This is another example of how scam artists are using the Internet to cheat consumers out of their hard-earned dollars," Spitzer said. "Internet users and all consumers must be on guard against unscrupulous businesses."

The judgment against Woodside was issued recently by Justice Abdus-Salaam of the New York County Supreme Court at the request of the Attorney General. The suit alleged the company violated New York consumer protection laws by misleading its clients and misrepresenting its services.

The Attorney General's office had received complaints from dozens of consumers, many of whom said they lost as much as $400 in fees to Woodside. The company lured would-be authors with glowing evaluations of writing samples, and then imposed steep charges for further review and processing of manuscripts.

Consumers who paid an initial reading fee of as much as $150 were informed that their work was "publishable." They were then asked to pay an additional $250 contract fee.

To lend credence to the scam, Woodside told authors that only five percent of submissions were accepted by the agency. In reality, the company offered contracts to anyone who paid the initial reading fee.

The Attorney General's Office investigated Woodside after receiving complaints from writers who grew tired of the company's repeated solicitations through literary-related news groups and bulletin boards.

In an effort to test Woodside's literary standards, a group of writers actually submitted a bogus writing sample that was filled with nonsensical prose, and grammatical and spelling errors. Woodside later requested the author's entire manuscript -- and a fee.

According to one Internet user, Woodside harassed writers who attempted to warn others of the scam, even threatening legal action in some cases.

"Most legitimate literary agencies look at a writer's work for free and only charge a fee if the book, short story or poem is sold. The agent then receives a percentage of the contract agreed upon by both parties," Spitzer said.

Consumers can still file complaints against the company with the Attorney General's office for possible restitution. The company has already been ordered to pay nearly $15,000 in penalties, restitution, and costs.

The case was handled jointly for the Attorney General by Assistant Attorney General Eric A. Wenger of the Internet Bureau and Assistant Attorney General Jane Azia, Deputy Chief of the Bureau of Consumer Frauds and Protection, with the assistance of Assistant Attorneys General Joy Feigenbaum and Melissa Saren.

Indice