

Internet : aspetti penali e criminologici

di :

Bruno Fiammella¹

Intervento al Convegno " Internet : fra diritto e tecnologia ", Lanciano, 17-18 maggio 2002.

Parlare di computer crime e di sicurezza oggi non è più una novità. Il sogno di una comunicazione globale e pervasiva è ormai una realtà grazie all'evoluzione tecnologica, alle reti cellulari e satellitari e ad internet. E' inconfutabile che tali nuove forme di comunicazione richiedano una tutela ben specifica e mirata ormai anche sotto il profilo legale. Parlare dal cellulare o mandare una e-mail non è ovviamente la stessa cosa rispetto al comunicare di persona, ma ciò che forse a molti di noi sfugge è che la tutela di queste nuove forme di comunicazione è ancora intrinsecamente molto bassa. Molto più bassa di quello che ci aspettiamo da una normale telefonata. Il problema quindi che la nostra collettività vive è quello di non avere ancora percepito, e raggiunto, la necessaria maturità sull'utilizzo di queste nuove tecnologie a causa della relativa gioventù delle stesse, non ha cioè ancora maturato una vera e propria cultura.² Noi non abbiamo sviluppato quei comportamenti innati di salvaguardia che in ogni individuo sono presenti fin dall'infanzia.

Per fare un esempio, un bambino in età scolare sa come attraversare la strada senza essere travolto da un'autovettura, sa che non deve accettare *avance* dagli sconosciuti e che non deve aprire la porta di casa a chiunque bussi. Un adulto oggi usa il computer con sufficiente difficoltà.

Se potevano esistere anni fa "dei dubbi sulla rilevanza - qualitativa ed in prospettiva quantitativa - del fenomeno della criminalità informatica, i recenti provvedimenti dell'autorità giudiziaria, hanno dimostrato come comportamenti penalmente rilevanti possano frequentemente presentarsi nell'ambito di attività imprenditoriali e professionali nei termini descritti dalle fattispecie normative".³

Il Csi (Computer Security Institute) ha presentato nel 2001 i risultati dello studio "Computer Crime and Security Survey". La ricerca è stata condotta in collaborazione con la Computer Intrusion Squad del FBI di San Francisco. Sulla base dell'esame delle risposte fornite da 538 responsabili della sicurezza elettronica appartenenti ad aziende, enti pubblici, università ed istituzioni finanziarie e ospedaliere, lo studio ha confermato che la minaccia costituita dai crimini elettronici e da altre falle nella sicurezza informatica rimanga estremamente elevata e il pedaggio in termini finanziari sta divenendo sempre più pesante.⁴

Il Consiglio dell'Unione Europea, nel mese di novembre 2001 a Budapest, ha emanato una documento sul cyber-crimine avente una finalità precisa : quella di sollecitare gli

Stati membri a perseguire una comune politica legislativa per proteggere il «villaggio globale» dai criminali informatici.

Ma il salto che si dovrà compiere è ben più alto : la sicurezza infatti non è solo un prodotto da vendere ma una cultura da acquisire. La sicurezza richiede progettualità, integrazione con i processi aziendali, consapevolezza, e necessità di una continua verifica a causa del fatto che lo stato dell'evoluzione è esso stesso, per sua natura, in continuo fermento.⁵

Parlare quindi di sicurezza è diventata una necessità non solo sociale ma anche e soprattutto economica. Le piccole e grandi aziende, le pubbliche amministrazioni utilizzavano fino ad ieri il ricorso all'esperto legale solo per gestire le cosiddette "situazioni di emergenza". Oggi stiamo passando dalla gestione delle emergenze alla cosiddetta prevenzione. Una corretta attività di *risk assessment* richiede un'analisi dei potenziali rischi a cui potrebbe essere soggetto il sistema informativo aziendale, le probabilità di accadimento, i danni che ne potrebbero derivare, i costi per rimediare o per prevenire gli eventi negativi.⁶

Una società aveva predisposto tutto il suo sistema con una cifratura di dati creando una gerarchia di accesso efficiente. Tuttavia questa società effettuava il *backup* dei dati ogni mese e li trasferiva in un ambiente diverso, con un unico particolare : questo *backup* era fatto in chiaro e lo trasportava un fattorino con una borsa non protetta nel luogo della azienda che fungeva da archivio. Un errore imperdonabile. Questo ci fa comprendere come mancasse una effettiva progettualità, una analisi del rischio. La sicurezza infatti è come una lunga catena che si compone di molteplici anelli. La reale efficacia di questa catena sta nel suo anello più debole; noi possiamo dotare i nostri sistemi di *firewall* o di *password* ma se non prestiamo attenzione a particolari come i floppy disk o i cd rom vanifichiamo ogni sforzo rendendo inefficienti gli investimenti compiuti per la sicurezza stessa del sistema. La sicurezza assoluta infatti non esiste ma è sempre qualche cosa che sottende una forma di equilibrio da cercare.⁷ La sicurezza delle reti e delle informazioni è infatti un problema evolutivo strettamente legato alla rapidità dei cambiamenti tecnologici che pongono continuamente nuove sfide.⁸

Cos'è allora il computer crime ?

E come possiamo identificare questa nuova sfera di cyber criminali ? "L'evoluzione tecnologica esercita una ampia forza di attrazione nei confronti di numerosi comportamenti delittuosi".⁹

La scienza criminologia ci insegna che le azione criminali non devono essere interpretate come il solo prodotto di pulsioni interne né vanno immaginate in un ambiente asettico ed ininfluente poiché in realtà esse risentono dell'attività del fitto "reticolo" socio-culturale che le circonda. Esse cioè sono il frutto di una molteplicità di fattori :quali l'ambiente esterno, il contesto sociale in cui il soggetto si è formato e vive, il rapporto con la vittima

e, non ultimo con sé stessi. L'autore del crimine infatti, prima di compiere un'azione criminosa, tende a rappresentarsi quello che sarà il frutto e la conseguenza della propria azione.¹⁰

E' possibile dare, in criminologia, una definizione di computer crime come l'insieme dei casi in cui " il computer si interpone tra l'autore del crimine e la vittima o comunque rappresenta lo strumento principale per eseguire una determinata azione criminale".¹¹ E' cioè importante evidenziare la capacità della macchina di alterare la percezione della gravità dell'azione criminale da parte dell'autore del crimine, la percezione della vittima, la stima dei rischi di essere scoperto e catturato. E' il fenomeno della cosiddetta spersonalizzazione. La distanza fisica tra l'autore e la cosiddetta scena *criminis* impedisce al soggetto di percepire la gravità di quanto sta compiendo.

La percezione del crimine, in ambiente digitale quindi è notevolmente distorta. In alcuni casi di pedofilia on-line le modalità di approccio dei pedofili nelle *chat* line evidenziano un'intuibile sottostima dei rischi di essere scoperti rispetto alle modalità di approccio classico del mondo reale. Questo elemento è molto importante perché ci permette di comprendere come i comportamenti tenuti tramite realtà virtuale abbattano i freni inibitori del soggetto che si ritrova a compiere azioni anche illecite che nella realtà, in modalità cioè face-to-face, non sarebbe in grado di effettuare.

Uno studio pilota sulle truffe condotte con le carte di credito ha evidenziato, da parte di soggetti completamente avulsi alle dinamiche criminali classiche, una maggiore "disponibilità al crimine" nel momento in cui questi stessi individui vengono proiettati in un contesto digitale, laddove la scena *criminis* si trasferisce tra i polpastrelli dell'autore e la tastiera, tra i suoi occhi e le emissioni elettromagnetiche del monitor.¹²

Chi sono allora questi nuovi criminali ? I cosiddetti cybercriminali comprendono una fenomenologia talmente diversificata da non poter essere più semplicemente ricondotta alla conosciuta figura degli hackers.

Questo termine è utilizzato impropriamente in quanto all'interno della comunità informatica la definizione di " hacker " ha sempre avuto una connotazione positiva, è solo recentemente che la stampa ed il giornalismo la utilizzano per identificare coloro che sfruttano le debolezze dei sistemi per causare intrusioni o danneggiamenti. Ad essere precisi, il termine appropriato per indicare tale comportamento è quello di "cracker" ossia distruttore, dal verbo to crack che significa "rompere, spezzare" La grande differenza quindi tra le due figure è che mentre i primi fanno irruzione per gioco o per scommessa, non dimentichiamo che gli hackers si definiscono una "elite" (Bruce Sterling), e comunque per dimostrare la loro superiorità rispetto al sistema, i secondi compiono vere e proprie razzie devastanti agendo anche per vendetta per personale o sociale o al fine di trarre profitto dalle loro azioni o di causare ad altri un danno.

CAM : una ricerca pilota dello IURC e dell'Università Cattolica di Roma

Vi presento il risultato di un caso di un giovane hackers che chiameremo "CAM", studiato attraverso un metodo di ricerca in corso di sperimentazione da parte del nostro Gruppo di ricerca sul computer crime dell'Istituto Universitario di Ricerche Criminologiche e dall'Università Cattolica del Sacro Cuore di Roma.

Lo strumento è stato somministrato al soggetto in modalità off-line (faccia a faccia).

Il soggetto è un maschio, ha 26 anni e non ha precedenti penali. E' giunto all'osservazione dei ricercatori grazie alla mediazione di un informatico professionista che lo conosce. Sembra apparire timido e un po' diffidente ma quando inizia il colloquio è felice di raccontare all'intervistatore la sua storia. Accetta di buon grado la somministrazione degli strumenti di indagine, mostrandosi interessato. La somministrazione dura circa due ore e mezza.

CAM è un soggetto che opera prevalentemente in solitario. Le sue competenze informatiche sono di livello medio-basso. Ha appreso alcune tecniche basiche che gli consentono di effettuare operazioni di hacking abbastanza semplici. Non sembra presentare tratti personologici particolari (se non una leggera introversione che però supera quando trova un interlocutore accettabile) o disturbi psicologici evidenti. La sua fruizione della tecnologia informatica non presenta carattere di ossessione o dipendenza. La sua vita relazionale off-line è infatti normale. E' consapevole dell'illegalità della sua condotta anche se non gli attribuisce carattere di particolare gravità. La percezione dei danni derivanti dalla sua attività di hacker è presente, anche se rielaborata attraverso operazioni di disimpegno morale. Le sue motivazioni principali, rispetto all'attività di hacking, sono legate al divertimento e alla sfida conoscitiva con le nuove tecnologie. Non si evidenziano infatti particolari spinte distruttive o vandaliche e le intrusioni vengono interpretate e significate prevalentemente come un mezzo di gratificazione dell'ego.

Io non sono uno psicologo, sono un legale, per me questa analisi significa che questo Hackers è una persona normale, è uno di noi ed è come tutti noi. Questo significa che i tratti comuni e gli stereotipi che possediamo in relazione ai comuni criminali, non sempre si adattano con la nuova categoria di cybercriminali.

Si è parlato di computer crime come *white collar crimes*, crimini dal colletto bianco, in realtà anche questo stereotipo, come quello del ragazzino punk con occhialini e capelli a spazzola deve essere superato.

I nuovi strumenti informatici sono ormai all'attenzione delle organizzazioni criminali, le esperienze processuali maturate in un ambiente che "respira di diritto penale" mi lascia affermare come gli errori in cui cadevano le organizzazioni pochi anni fa sono ormai relegate a vicende processuali che stanno facendo il loro corso; la linea ISDN era considerata tanto sicura da ritenere che le comunicazioni su di essa non fossero intercettabili così da sviluppare tramite essa procedimenti e comunicazioni finalizzate alla

clonazione di titoli di credito. I circuiti bancari telematici sono senza dubbio il nuovo oggetto di attenzione per la criminalità organizzata. Il trasferimento elettronico di fondi e l'attività finanziaria virtuale richiedono degli strumenti investigativi potenziati e delle procedure semplificate a livello transnazionale, e di fronte a queste legittime richieste degli organi investigativi, occorre che il difensore sia altrettanto esperto e preparato e che affianchi, alla preparazione giuridica ed all'esperienza professionale, anche una sufficiente conoscenza della tecnologia informatica, diventando anche questo un campo in cui il professionista diligente non può più rispondere con approssimazione. Nuova frontiera, nel campo della criminalità è invece costituita da un movimento legato alla cosiddetta bio-informatica (cioè applicare l'informatica alla biologia per elaborare i progetti di mappatura dei genomi). Nascono i cosiddetti "hackers biologici". Questi soggetti aderiscono al principio dell' "Acces to research", cioè alla condivisione delle informazioni legate ai risultati delle ricerche relative ai brevetti sui geni.

Ma il vero pericolo attuale è costituito dalle figure come quella dell'insider semplicisticamente definito dipendente infedele. Chi lo ha detto che sia un dipendente e non un manager ? L'attività di social ingeneriing (che è una tecnica effettuata attraverso tranelli psicologici, inganni, nei confronti di un soggetto per ottenere a sua insaputa una serie di informazioni necessarie per l'accesso al sistema) può essere utilizzata da chiunque, anche da che si trova ai cosiddetti "piani alti" della gerarchia aziendale.

La tutela del bene informatico

In dottrina si parla di un nuovo bene giuridico : il bene informatico. E' presente in alcune giovani Costituzioni, per esempio negli articoli 18 e 105 della Costituzione Spagnola del 1978 e nell'articolo 35 di quella Portoghese del 1976.

In Italia il provvedimento legislativo che fa riferimento alle ipotesi di criminalità informatica è la legge 23 dicembre 1993 n° 547 intitolata «Modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica», con essa anche l'Italia si è messa al passo con i tempi dotandosi di una legislazione penale dell'informatica.

La legge è composta di 13 articoli (tre dei quali riguardanti la procedura penale) che introducono nuove ipotesi di reato all'interno del codice penale o ampliano la portata di quelle già esistenti. Si è quindi optato per una soluzione di modifica al codice penale esistente piuttosto che alla creazione di un autonoma legge speciale.

Con il termine reato informatico si vuole indicare qualsiasi condotta realizzata per mezzo delle nuove tecnologie o rivolta contro beni informatici e sanzionata dall'ordinamento penale. Dobbiamo però distinguere i casi in cui il reato è compiuto attraverso il computer (ad esempio frode informatica) da quelli in cui il computer è il bene leso (esempio il danneggiamento). Nella prima ipotesi le tecnologie sono strumento di reato, nel secondo caso invece sono oggetto di tutela dai reati, come strumento di reato possono ledere sia

se stesse, e quelli che sono stati definiti "beni informatici", e sia molti beni giuridici tradizionali che anche attraverso le tecnologie si esprimono.

Accesso abusivo ad un sistema informatico o telematico

La salvaguardia dei sistemi informatici dall'accesso abusivo costituisce uno degli aspetti più complessi e delicati della criminologia informatica e trova la sua genesi nel momento in cui l'evoluzione tecnologica ha consentito a più computer o a più sistemi di "dialogare" tra loro.¹³

Cosa tutela la norma ? Una nuova esigenza di salvaguardia, quella del proprio domicilio informatico, questo nuovo spazio virtuale costituito prevalentemente da informazioni, spazio in cui si esplica la personalità del singolo. La necessità di tutelarsi dall'accesso abusivo, infatti, implica il riconoscimento dell'esistenza di un nuovo "spazio virtuale" costituito e delimitato non più da elementi di tipo "fisico" quali le mura di un edificio ma da "informazioni".

Del domicilio conosciamo i tradizionali concetti : la giurisprudenza ha pedissequamente accompagnato l'evoluzione, arrivando ad inglobare, in questa definizione, oltre alle mura domestiche, anche l'auto, la roulotte, la banca, fino ad arrivare, alla più recente definizione di domicilio informatico.

L'art. 615 *ter* c.p., punisce chiunque si introduca senza autorizzazione in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantenga contro la volontà esplicita o tacita di chi ha il diritto di escluderlo.

La norma recita testualmente : "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero si mantiene contro la volontà di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni".

Il comportamento incriminato consiste nell'introdursi abusivamente all'interno di un sistema e nel mantenersi. Tuttavia il legislatore ha specificato nella formulazione della fattispecie le due condotte in forma distinta e separata. Questo perché noi potremmo essere autorizzati ad entrare in un sistema, ad esempio per scrivere o leggere alcuni dati, ma potremmo anche, successivamente al compimento dell'attività per la quale siamo stati autorizzati, mantenerci indebitamente all'interno della macchina, del computer e compiere tutta una serie di operazioni per le quali non siamo stati esplicitamente o implicitamente autorizzati.

Questa condotta è facilmente riscontrabile nei luoghi di lavoro dove, l'intervento temporaneo sulla macchina del collega, si rivela uno dei momenti più a rischio per l'integrità del sistema stesso.

La condotta commissiva dell'accesso abusivo è dovuta al fatto che la norma è costruita sul volontario mantenimento dell'accesso nonostante il divieto espresso o tacito del titolare.¹⁴

La fattispecie penale in questione restringe tuttavia il suo campo di azione ai soli casi di accesso ad un sistema informatico o telematico che sia protetto da "misure di sicurezza". L'intenzione del legislatore, è quella cioè di punire soltanto ove il titolare del sistema abbia dimostrato, attraverso l'inserimento di una misura di sicurezza, il cosiddetto "*ius excludendi alios*", la volontà di riservare l'accesso solo a persone da lui autorizzate. E' importante sottolineare come non è la qualità dei contenuti che giustifica il diritto alla riservatezza, ma è il fatto che comunque si tratti di un'area riservata.

Ma cosa sono quindi queste misure di sicurezza di cui ci parla la legge, quali sono cioè, all'atto pratico, gli strumenti che abbiamo per difenderci : si distinguono in misure fisiche (come la vigilanza), logiche (password), biometriche (lettura dell'iride o dell'impronta digitale, riconoscimento vocale). Su questo punto, quello delle misure di sicurezza vi è tuttavia un importante elemento da sottolineare : la scelta del legislatore di indirizzare la tutela penale solo per i sistemi dotati di misure di protezione. Tale scelta, male viene accolta da chi considera ingiustificata la distinzione dei vari domicili informatici. Si verrebbero cioè a creare sistemi protetti (di serie A) e sistemi non protetti (di serie B).

L'accesso al sistema diventa quindi abusivo ed illegittimo solo in presenza di un *quid pluris* che ci allerta sulla presenza di una *voluntas excludendi* da parte del titolare, una volontà di sbarramento manifestata in modo non equivoco.¹⁵ Su questo punto la Corte di Cassazione¹⁶ ha ritenuto che ciò che sia determinante per la configurazione del reato, non è tanto la presenza di misure di protezione interne o esterne al sistema, quanto l'aver agito contro la volontà contraria di chi dispone legittimamente del sistema.

Risvolti processuali

Oltre agli aspetti di tipo sostanziale, sono altrettanto interessanti i risvolti che esistono sotto il profilo processuale.

L'interazione infatti tra il processo penale ed i computer crimes si manifesta sia nella fase di accertamento dei reati informatici in senso stretto, sia in tutte quelle situazioni in cui il computer o la rete non sono stati utilizzati per commettere l'illecito penale, e tuttavia, contengono elementi probatori rilevanti.¹⁷

Le prime problematiche sono evidenti a tutti ormai : la dimensione sovranazionale ed a-territoriale del cyberspazio che, oltre a rendere impervia la ricerca delle prove, apre problematiche relative al momento consumativo del reato ed alla legge penale applicabile. Tutto ciò in parte ha anche causato una recente crisi di identità del diritto penale se inteso come un *corpus* di regole viventi ed identificate in una comunità sociale stanziata su un determinato territorio. Se è vero che "*ubi societas hominum ibi ius*" la domanda da porsi è allora di quale società parliamo quando ci riferiamo al cyberspazio? Le necessità quindi che sorgono sono relative al fatto che il sistema penale interno non può non essere in armonia con gli altri ordinamenti processuali, così come recentemente espresso dalla Convenzione del Consiglio d'Europa sul cyber-crime.

L'acquisizione delle fonti di prova è uno dei momenti più importanti e delicati nella fase delle indagini preliminari. Anni fa le conoscenze degli agenti di Polizia Investigativa erano sicuramente ridotte, oggi esistono dei reparti specializzati ed attrezzati anche sotto il profilo tecnico.

L'invasività che sempre un provvedimento di perquisizione e sequestro emesso dall'A.G. comporta, seppure indispensabile, in quanto momento cardine dell'acquisizione delle fonti di prova, dovrebbe essere temperata da comportamenti e conoscenze tecniche tali da ridurre al minimo il disagio per l'attività lavorativa del singolo o dell'azienda.

Esempio ormai classico: alle sacrosante proteste apparse su riviste del settore che lamentavano il sequestro dell'intero server dedicato ad ospitare i siti WEB di centinaia di clienti di un Provider ed altri servizi ancora, operato dalla Polizia Giudiziaria, al fine di acquisire ed impedire la diffusione di un messaggio diffamatorio, laddove sarebbe stata possibile la "rimozione" del solo sito o del solo messaggio diffamatorio consentendo quindi ad una elevata pluralità di utenti non coinvolti dalle indagini l'utilizzo di servizi e prestazioni legittime ed indispensabili alle loro attività.

Altro comportamento, di cui soprattutto le aziende si lamentano, è quello causato dalla mancata conoscenza di tecniche meno invasive di acquisizione della fonte di prova, che induce la polizia giudiziaria, operante in presenza di software illecitamente duplicato, a sequestrare il computer comprensivo di video e periferiche laddove sarebbe sufficiente (dandone atto a verbale) riversare su altro supporto magnetico fornito dalla parte l'intero contenuto dell'HD incriminato, rimuovendo poi dall'Hard Disk che rimane in disponibilità dell'azienda il solo software illecitamente duplicato.

Questa non difficile operazione consentirebbe all'azienda di poter continuare ad operare utilizzando il software ed i dati che legittimamente detiene senza dover interrompere le attività produttive, ed all'autorità Giudiziaria di acquisire le fonti di prova senza penalizzare eccessivamente l'attività lavorativa e produttiva e senza venire a conoscenza di informazioni contenute nello stesso hard disk che per l'azienda possono comunque assumere a livello concorrenziale, un rischio qualora fossero indebitamente divulgate.¹⁸

Sotto questo profilo, è interessante segnalare una sentenza del Tribunale del riesame di Torino di due anni fa che determinò un'inversione di tendenza nella giurisprudenza, Proprio in relazione ai sequestri, il tribunale asserì, accogliendo su questo punto il ricorso presentato dalla parte, come non fosse necessario effettuare il sequestro dell'intero hard disk. "Nulla impediva agli agenti di p.g., appartenenti alla Sezione specializzata nell'ambito dei reati informatici, di procedere ad una copia integrale dell'hard disk, con specificazione verbale di ogni singola operazione". Non è necessario asserisce il tribunale, "mantenere ulteriormente il sequestro, con compressione delle legittime aspettative del possessore dell' hard disk, tenuto soprattutto conto che appare altamente verosimile che vi siano una serie di e-mail che potrebbero non concernere la fattispecie di reato

contestata, e-mail che avrebbero dovuto essere restituite immediatamente. Il mantenimento del sequestro dopo un tempo apprezzabile appare non consentito, spettando agli agenti già in sede di perquisizione, ovvero al consulente nominato ex 'art. 359 c.p.p. o 360 c.p.p. una immediata selezione del materiale rilevante, ancor prima delle successive operazioni peritali".

E' altrettanto doveroso segnalare un altro legittimo aspetto che si contrappone alle richieste delle autorità e di coloro che operano nella settore della sicurezza : un ulteriore problema cioè risiede nel fatto che la maggior parte delle vittime di reati informatici non riporta i casi, non denuncia quanto accaduto, rendendo ancora più difficile quindi quantificare precisamente l'ammontare dei danni provocati dai criminali che utilizzano la rete per le loro attività illecite.

Le ragioni che stanno alla base della decisione di non denunciare i reati informatici sono molteplici e differenti. Per le aziende in alcuni casi si tratta semplicemente di una decisione economica, di un calcolo costi benefici: il danno può risultare di importanza secondaria, tale da non giustificare l'impiego di energie e risorse necessarie ad attivare un'indagine. Un'altra ragione può risiedere nel fatto che l'effetto della notizia del reato informatico possa in qualche modo diminuire il valore dell'impresa che l'ha subito, e in questo caso si può decidere di gestire il problema internamente. Infine, una precisa scelta politica dell'azienda : alcune imprese sono consapevoli del fatto che una cattiva pubblicità potrebbe generare allarme nel pubblico e, soprattutto, che la notizia della vulnerabilità dei propri sistemi informatici potrebbe incoraggiare altri attacchi da parte dei pirati informatici.¹⁹

Certo, in questa materia le certezze sono ancora poche ed i dubbi molti, ma è proprio questo, a mio avviso, che ci deve spingere ad un continuo confronto, proprio perché il prossimo futuro vedrà sempre più vicine le figure del legale e dell'esperto di tecnologie informatiche, lasciando a ciascuno il relativo campo di competenza, ma anche creando una nuova ed indispensabile sinergia tra le due figure professionali.

¹ Direttore sede IURC (Istituto Universitario di Ricerca Criminologia) di Reggio Calabria, curatore del sito www.fiammella.it ;

² **Corrado Giustozzi** : *Il problema della sicurezza informatica*, 2001

³ **Cesare Parodi** : *La tutela penale dei sistemi informatici e telematici: le fattispecie penali*, Relazione presentata al Convegno Nazionale su 'Informatica e riservatezza' del CNUCE - Pisa 26/27 settembre 1998.

⁴ CSI: Aumentano i danni economici detrivanti da intrusioni, spionaggi industriale e crimini elettronici commessi via Internet

⁵ **Giuseppe Casarano** : *Sicurezza informatica : Non solo prodotti* in Atti del convegno : *Computer crime*, CNEL, 27 aprile 2000.

⁶ **Giuseppe Luca, Mantese Matteroni** : *Sicurezza informatica : guida per l'azienda*, pag. 8, Milano, 2000.

⁷ **Giuseppe Casarano** : *Sicurezza informatica : Non solo prodotti* in Atti del convegno : *Computer crime*, CNEL, 27 aprile 2000.

⁸ Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle Regioni : *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*.

⁹ **Francescopalolo Ruggiero** : *Momenti consumativi del reato e conflitti i giurisdizione nel Cyberspazio*, Giurisprudenza di Merito, vol. XXXIV, Gennaio - Febbraio 2002

¹⁰ **Marco Strano** : *Le subculture devianti nel cyberspazio*, January 2001, in www.criminologia.org; vedi anche *Relazioni digitali e comportamenti devianti*, relazione al convegno "Psichiatria, informatica e telemedicina. Realtà e prospettive nel campo dell'assistenza e della formazione". Velletri, sala Micara, 29 marzo 2001 in www.criminologia.org

¹¹ **Marco Strano** : *Psicologia del computer crime*, in Atti del convegno : *Computer crime*, CNEL, 27 aprile 2000.

¹² **Marco Strano** : *Relazioni digitali e comportamenti devianti*, relazione al convegno "Psichiatria, informatica e telemedicina. Realtà e prospettive nel campo dell'assistenza e della formazione". Velletri, sala Micara, 29 marzo 2001 in www.criminologia.org

¹³ **Paolo Galdieri** : *Teoria e pratica nell'interpretazione del reato informatico*, 1997, Giuffrè

¹⁴ **Pica Giorgio** : *Diritto Penale delle Tecnologie informatiche*, 1999, UTET

¹⁵ **Pica Giorgio** : *Diritto Penale delle Tecnologie informatiche*, 1999, UTET

¹⁶ Corte di Cassazione Sez. V. n. 1675/2000

¹⁷ **Luparia Luca** : *Computer crime e processo penale*, Internet Cyber Law Conference, Bologna, 29 novembre 2001

¹⁸ **Gianfranco Todesco** : *L'Indagine Informatica di Polizia Giudiziaria: trasmissione dati su rete, perquisizioni ed ispezioni informatiche* (Relazione presentata al Convegno Nazionale su 'Informatica e riservatezza' del CNUCE - Pisa 26/27 settembre 1998).

¹⁹ **Charney & Alexander** : tratto da : Relazione presentata al convegno: "*La questione criminale nella società globale*" Napoli, Italia, 10 - 12 dicembre, 1998.