Il computer crime e le strategie di contrasto

di *Luciano Rosini*[1]

Riassunto
Lo sviluppo di Internet, dal quale derivano rilevanti opportunità di crescita in numerosi ambiti, ha ridefinito la quotidianità, rendendola sempre più strettamente connessa all'impiego di nuove tecnologie. Tuttavia, a fronte degli innegabili vantaggi ed aspetti positivi, si profilano altresì nuove forme di criminalità attuate nel cyber-spazio capaci di evidenziare le debolezze dei sistemi legislativi e delle modalità investigative tradizionali. In particolare, la minaccia criminale nel mondo virtuale ha assunto oggi una connotazione transnazionale, collocandosi in un "luogo" non più configurabile entro i confini territoriali dei singoli Stati. Allo scopo di fronteggiare adeguatamente siffatti pericoli, nel 1998 è sorto in Italia il Servizio Polizia Postale e delle Comunicazioni, il quale rappresenta il risultato di un processo di adeguamento delle strutture investigative nazionali in grado di rispondere alle minacce conseguenti simili mutamenti di ordine tecnologico e culturale.

Abstract
The development of Internet, has opened opportunities of growth in many sectors, and has redefined daily life, making it more and more closely connected to the implementation of new technologies. Nevertheless, apart from the evident positive aspects, new forms of criminality are appearing in the cyber-space, able to show up the weaknesses of our normative systems as well as of the traditional investigative procedures. In particular, today the "virtual" criminal threat has become transnational, occupying a "place" that is no longer confined within national bounderies. In order to cope with dangers and risks, in 1998 in Italy the "Servizio Polizia Postale e delle Comunicazioni" was founded. The aim is to make our investigative procedures conform to international standards, so as to provide an appropriate answer to all the threats coming from such techonological and cultural transformation.

1. Introduzione.

Sono il Prefetto Luciano Rosini, direttore della Direzione Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato. Ho assunto questo incarico da oltre un anno, dopo una ventennale esperienza maturata, in varie città d'Italia, nel contrasto al crimine comune ed organizzato. Nel ringraziare per il cortese invito che mi è stato rivolto ad intervenire oggi quale relatore del convegno organizzato dall'Università di Bologna, vorrei rilevare che sono particolarmente lieto di essere qui per due diversi motivi. Infatti, se da un lato sono onorato di essere parte dei un processo formativo che conferma la storica tradizione formativa di grande qualità dell'Università di Bologna, d'altro canto sono contento di cogliere l'opportunità di

[1] Prefetto, Direttore della Direzione Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato.

illustrare le linee strategiche del Dipartimento della Pubblica Sicurezza adottate per un migliore contrasto dei fenomeni di criminalità informatica.

Intervengo in questa sede portando a tutti voi il saluto del Prefetto Gianni De Gennaro, Direttore Generale della Pubblica Sicurezza, il quale segue con attenzione lo svolgimento dei lavori di questo convegno e sarà mia cura aggiornarlo degli esiti raggiunti.

All'interno della complessa ed articolata Direzione Centrale che ho l'onore di dirigere, il compito del contrasto ai fenomeni di criminalità informatica transnazionale è assolto dal Servizio Polizia Postale e delle Comunicazioni diretto dal Dirigente Superiore della Polizia di Stato Dottor Domenico Vulpiani.

Il Servizio Polizia Postale e delle Comunicazioni rappresenta il risultato di un processo di adeguamento delle strutture investigative nazionali per meglio affrontare le minacce derivanti dall'ingresso delle nuove tecnologie in ogni ambito della società civile ed in particolare in quello della comunicazione.

Il Dipartimento della Pubblica Sicurezza, sin dal 1998, ha avvertito l'esigenza di dedicare al contrasto di queste nuove forme di criminalità, una struttura specialistica quale il Servizio Polizia Postale e delle Comunicazioni, individuata successivamente, con apposito decreto, quale "*organo per la sicurezza e la regolarità dei servizi delle telecomunicazioni*".

Più precisamente il Servizio Polizia delle Comunicazioni è stato istituito con decreto del Ministro dell'Interno del 31 marzo 1998 nell'ambito di una riorganizzazione più complessa che ha coinvolto tutte le Specialità della Polizia di Stato gestite dalla Direzione Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato.

L'obbiettivo della riforma e' stato quello della razionalizzazione delle risorse impegnate all'interno del Dipartimento di Pubblica Sicurezza nel contrasto alle attività illecite commesse attraverso l'utilizzo dei nuovi *media*, con la costituzione di un *pool* di professionisti impegnati nelle investigazioni contro i crimini informatici. Raccogliendo la necessità di individuare una Forza di polizia cui attribuire, per le sue peculiarità istituzionali, il compito specifico di far fronte alla nuova minaccia criminale, venne concepita la Polizia Postale e delle Comunicazioni che, tra le Specialità della Polizia di Stato, è quella che maggiormente è stata interessata nel corso degli anni dalle dinamiche evolutive della sfera delle proprie attribuzioni.

Istituita nel 1981[2] al fine di provvedere alla tutela di quanto tradizionalmente veniva definito *servizi postali e delle telecomunicazioni*, nel 1984[3] vede attribuirsi specifiche competenze, soprattutto in materia informatica e di comunicazioni elettroniche, determinate dal rapido e continuo progresso tecnologico, dall'avvento della cd. *società dell'informazione* e di *Internet*, così come dalla sopra indicata evoluzione degli stessi fenomeni criminali nei medesimi settori.

[2] Art. 34 L. 01.04.1981 n. 121 - "Nuovo ordinamento dell'Amministrazione della Pubblica sicurezza", istitutivo degli Uffici di Polizia Stradale, Ferroviaria, Postale e di Frontiera

[3] Art. 1 D.M. 14.08.1984 "Organizzazione dei servizi sulla polizia postale"

Nel 1992[4], alla Polizia di Stato viene affidata la competenza nelle indagini in materia di *criminalità informatica* e di *attività illecite nel settore dell'elettronica* e, nel 1993[5], le importanti innovazioni legislative in materia di criminalità informatica inducono il Dipartimento di P.S. al consolidamento delle funzioni di prevenzione e repressione nel settore delle *comunicazioni non solo postali ma anche radio, televisive, telefoniche e telematiche*, tanto che nel 1996[6] viene istituito il N.O.P.T. – Nucleo Operativo di Polizia delle Telecomunicazioni, quale *organo di supporto tecnico investigativo nelle attività di indagine particolarmente complesse, nel campo della telematica e dell'informatica*, composto da qualificati investigatori provenienti dalla Direzione Centrale della Polizia Criminale. Nell'ambito di una complessa riorganizzazione che ha coinvolto tutte le Specialità della Polizia di Stato, nel 1998[7] viene infine istituito il Servizio Polizia Postale e delle Comunicazioni, quale *pool di professionisti* specializzati nelle attività di contrasto dei fenomeni delittuosi nel loro insieme compresi nel più ampio concetto di *cyber crime* oltre che deputati alla prevenzione ed al contrasto dei reati in materia di servizi postali e delle comunicazioni in genere.

A tale sforzo organizzativo ed all'efficacia dei risultati operativi conseguiti, in breve tempo verranno conferiti importanti riconoscimenti: nel 1998[8], al personale specializzato del Servizio vengono affidate, per alcuni aspetti in via esclusiva, competenze in materia di contrasto alle *condotte di induzione alla prostituzione minorile, produzione, commercio, cessione, distribuzione e divulgazione di materiale a contenuto pedo pornografico, consumate mediante l'impiego di sistemi informatici o mezzi di comunicazione telematica e reti di telecomunicazione pubbliche***;**

nel 1999[9], il Servizio viene invece individuato quale Organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni;

nel 2005[10], allo stesso Servizio vengono affidate in via esclusiva competenze, di primaria rilevanza, in

[4] Art. 4.7 D.M. 22.01.1992 "Direttive per la definizione delle linee di prevenzione anticrimine e per le attività investigative di cui all'art. 1 c.2° lett. A D.L. 345/91 conv.to in legge 410/91"

[5] L. 23.12.1993 n. 547 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"

[6] 18.05.1996 - "Atto dispositivo del Capo della Polizia – Direttore Generale della p.s. "

[7] D.M. 31.03.1998, istitutivo – nell'ambito della Direzione Centrale delle Specialità della Polizia di Stato - del Servizio Polizia Postale e delle Comunicazioni, facendovi confluire il personale della preesistente Divisione Polizia Postale e del N.O.P.T.

[8] L. 03.08.1998 n. 269 recante "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali forme di riduzione in schiavitù", il cui art. 14, comma 2°, prevede che:
"*Nell'ambito dei compiti di polizia delle telecomunicazioni..... l'organo del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazione svolge, su richiesta dell'Autorità giudiziaria, motivata a pena di nullità, le attività occorrenti per il contrasto dei delitti di cui agli artt. 600 ter c. 1,2,3, e 600 quinquies del codice penale commessi mediante l'impiego di sistemi informatici o mezzi di comunicazione telematica ovvero utilizzando reti di telecomunicazione disponibili al pubblico. A tale fine il personale addetto può utilizzare indicazioni di copertura, anche per attivare siti nelle reti, realizzare o gestire aree di comunicazione o scambio su reti o sistemi telematici, ovvero per partecipare ad esse. Il predetto personale specializzato effettua con le medesime finalità le attività di cui al comma 1(n.d.r.: acquisto simulato di materiale pedo pornografico, attività di intermediazione, partecipazione ad iniziative turistiche di cui all'art. 5 della stessa legge), anche per via telematica. "*

[9] D.I. 19.01.1999, istitutivo anche della Sezione distaccata presso l'Autorità per le Comunicazioni

[10] D.L. 27.07.2005 n. 144, convertito con modificazioni in L. 31.07.2005 n. 155, recante "Misure urgenti per il contrasto al terrorismo internazionale", il cui art. 7 bis, intitolato "Sicurezza telematica", al primo comma prevede che:
"*Ferme restando le competenze dei Servizi informativi e di sicurezza……l'organo del Ministero dell'Interno per la*

materia di *contrasto alle attività di terrorismo realizzate attraverso mezzi informatici*, con riferimento specifico:

- ai servizi di prevenzione e repressione del crimine informatico consumato (non soltanto per finalità di terrorismo) in danno dei sistemi delle Infrastrutture critiche che erogano o gestiscono servizi strategici per la sicurezza e la prosperità della Nazione,
- a strumenti di indagine particolarmente incisivi quali le intercettazioni preventive di flussi telematici e le attività investigative condotte con modalità sottocopertura.

Nel febbraio 2006[11], infine, il Legislatore istituisce, presso la Polizia delle Comunicazioni, del Centro Nazionale per il contrasto della pedopornografia sulla rete Internet. La Polizia Postale e delle Comunicazioni opera in tutto il Territorio Nazionale e può contare su circa 2000 investigatori specializzati nel contrasto alle problematiche connesse ai crimini informatici, impiegati sia a livello centrale che periferico. Il Servizio, coordina infatti l'attività di 19 compartimenti regionali e 77 sezioni provinciali. Funge inoltre da punto di contatto nazionale per le emergenze transnazionali in tema di reati informatici in conformità con la specifica rete 24 ore su 24, 7 giorni su 7 del G8.

Sono state anzi citati i recenti interventi legislativi hanno accresciuto le competenze del Servizio affidando il compito esclusivo della Protezione delle Infrastrutture Critiche Informatiche e della gestione del Centro Nazionale per il contrasto della Pedofilia su Internet.

L'utilizzo sempre più esteso dell'alta tecnologia nella società moderna crea nuove opportunità di sviluppo nelle aree di mercato economiche e finanziarie connesse ai nuovi media. Purtroppo, parallelamente, si aprono nel contempo nuovi scenari virtuali dove gruppi terroristici e criminalità comune o organizzata possono operare più facilmente, sfruttando le debolezze intrinseche dei sistemi o dell'essere umano, per ricavarne ulteriori, illeciti profitti o garantirsi una maggiore impunità.

Lo sviluppo di internet, da cui derivano opportunità enormi di crescita in campo sociale, economico, politico, culturale e scientifico, ha ridisegnato il nostro vivere quotidiano legandolo sempre più all'uso delle nuove tecnologie.

La velocità con cui tutto ciò sta accadendo, se da una parte accelera i processi positivi della nuova era, dall'altra scopre le debolezze dei sistemi legislativi ed investigativi tradizionali che stentano a tenere il passo per adeguarsi alle nuove realtà.

Ed ecco quindi che concetti ormai consolidati nel tempo quali quello della giurisdizione e la competenza territoriale vacillano di fronte a

sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'Interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.", mentre al secondo comma dispone che:

"*Per le finalità di cui al comma 1 e per la prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo condotte con mezzi informatici, gli Ufficiali di polizia giudiziaria appartenenti all'organo di cui al comma 1 possono svolgere le attività di cui all'art. 4, commi 1 e 2, del D.L. 18.10.2001 n. 374, convertito con modificazioni dalla L. 15.12.2001 n. 438, e quelle di cui all'art. 226 delle norme di attuazione, coordinamento e transitorie del codice di procedura penale, di cui al decreto al D.L.vo 28.07.1989 n. 271, anche a richiesta o in collaborazione con gli organi di polizia giudiziaria ivi indicati.* "

11 L. n. 38 del 6 febbraio 2006, recante "*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la*

situazioni che solo fino a pochissimo tempo fa erano lontani dalla mente persino del più fantasioso dei legislatori.

L'utilizzo della rete per finalità illegali è ormai realtà quotidiana. Anche il mondo virtuale, così come quello reale, è popolato da varie tipologie di delinquenti: da quelli molto pericolosi a quelli meno; da quelli che operano nel settore dei reati contro il patrimonio a quelli che attentano alle libertà individuali; dal delinquente solitario alle organizzazioni criminali più complesse come quelle a cui si faceva prima riferimento.

Andando oltre, i modelli organizzativi adottati oggi dalla società dell'informazione, sono ormai divenuti strumenti irrinunciabili della nostra stessa esistenza.

L'esperienza già vissuta dei disastrosi effetti degli attacchi terroristici e di alcuni *blackout* energetici che già hanno colpito tutto il mondo mettendo in luce tutte le vulnerabilità dei sistemi di controllo e di gestione delle crisi, ad esempio, è stata la triste occasione per sottolineare quanto il nostro vivere quotidiano sia assolutamente dipendente non solo dall'energia ma dell'intero sistema di comunicazioni sempre più globale.

Il superamento dei modelli tradizionali di spazio e di tempo, insieme con il vorticoso progresso tecnologico, costituisce il territorio favorevole perché nuove realtà criminali possano affacciarsi. Si tratta di realtà con le quali da tempo abbiamo a fare i conti e che genericamente ricadono sotto la denominazione di *cybercrime*.

La minaccia criminale nel mondo virtuale assume sempre più una connotazione transnazionale, svincolata dai confini dei singoli Stati. La caratteristica peculiare è la "distanza" tra i *cyber*criminali e le loro vittime potenziali.

La condotta delittuosa può concretizzarsi in più azioni svolte in tempi diversi o contemporaneamente, da più soggetti o da uno solo, in luoghi diversi o in uno spazio virtuale. Possono essere colpiti immediatamente o a distanza di tempo una o più vittime in uno o più luoghi.

E' altresì tristemente noto come organizzazioni criminali o terroristiche possano sfruttare le potenzialità comunicative della rete per comunicazioni individuali "in tempo reale", oltre che per attività di proselitismo, propaganda, reclutamento e raccolta di mezzi di sostentamento, sia finanziari che strumentali.

Sul fronte delle strategie di contrasto, la risposta dei governi impegnati ad assicurare allo spazio virtuale un livello di sicurezza adeguato deve puntare su una progettualità in cui i protagonisti siano le istituzioni e allo stesso tempo la società civile.

L'attività preventiva e repressiva dei reati commessi attraverso la rete internet però è fortemente ostacolata dalla difficoltà di identificare i fornitori/utenti e di localizzare i siti e i dati.

E' innegabile che internet sia stato e possa essere il volano per la diversificazione dei crimini. E' altresì evidente che le organizzazioni criminali e terroristiche stanno traendo giovamento dalle possibilità offerte dalla rete per migliorare la loro efficienza operativa e le loro capacità di sottrarsi alle indagini.

Per questi motivi, una strategia efficace di contrasto allo specifico fenomeno criminale dovrebbe seguire un percorso finalizzato al perseguimento dei seguenti obiettivi:

pedopornografia anche a mezzo Internet".

- armonizzare a livello internazionale le normative di settore;
- sviluppare la cooperazione, sia a livello giudiziario che di polizia;
- istituire corpi specializzati di polizia nel contrasto al crimine informatico;
- condividere la formazione tecnico-operativa a livello internazionale;
- collaborazione stretta fra organi deputati alla sicurezza dei sistemi informatici e gli operatori di polizia;
- costituzione di organismi nazionali ed internazionali deputati alla promozione delle politiche di sicurezza al fine di studiare la vulnerabilità delle infrastrutture critiche e sviluppare un sistema di protezione omogeneo.

Un notevole passo in avanti è stato fatto proprio con la sottoscrizione della Convenzione sulla Criminalità Informatica del Consiglio d'Europa ed al riguardo auspico la prossima conclusione, da parte dell'Italia, delle procedure di ratifica in corso.

Mi è gradito ricordare che la Convenzione[12] reca specifiche norme che, oltre a prevedere la conservazione e la custodia dei dati di traffico, prevedono anche le modalità della concreta cooperazione internazionale fra le quali, ad esempio, le disposizioni relative alla rete dei punti di contatto 24/7. Come si evince dai lavori preparatori, queste norme sono state redatte con chiaro riferimento e traendo beneficio dalle esperienze operative maturate in ambito G 8.

Proprio sul piano della cooperazione internazionale di polizia, nei giorni scorsi, il 17 ottobre, ho avuto il piacere di aprire i lavori della Seconda Conferenza Internazionale di Addestramento dei Punti di Contatto Operativi appartenenti alla Rete 24/7 del G8. La rete, che nel 1998 contava 8 Paesi, consente attualmente a ben 45 Paesi di essere collegati e di trasmettere in tempo reale le informazioni operative per il contrasto del crimine informatico transnazionale.

L'incontro, frutto di una iniziativa italiana al G8, è stato organizzato per la seconda volta dalla Polizia delle Comunicazioni che, pertanto, si è vista riconoscere anche dalla comunità internazionale il ruolo di *leader* dell'addestramento sulle materie di specifica competenza.

La rete, nata per la necessità di scambiare informazioni in tempo reale, ha avuto un considerevole impulso di operatività soprattutto in conseguenza degli episodi terroristici internazionali, dall'attacco alle torri gemelle negli Stati Uniti dell'11 settembre 2001, delle bombe nella ferrovia di Madrid del marzo 2004, alle bombe nella metropolitana di Londra del 7 luglio 2005.

Gli eventi citati, risultato di una mirata follia omicida, sono una triste e terribile testimonianza del fatto che le organizzazioni terroristiche sono in grado di colpire, non solo i singoli Stati, ma l'intera umanità.

Nel premettere che tali atroci accadimenti devono essere un monito per tenere alta la guardia e l'impegno per combattere, sempre con vigore, il crimine organizzato transnazionale in tutte le forme in cui esso si manifesta, auspico che la mia partecipazione a questo convegno, insieme con

[12] Disponibile alla pagina:
http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc

quella del Dottor Vulpiani, possa contribuire ad accrescere gli sforzi che ognuno di noi può compiere contribuendo, per la sua quota parte, alla promozione di una complessa cultura globale della sicurezza.