La nuova criminalità informatica.
Evoluzione del fenomeno e strategie di contrasto.

Domenico Vulpiani[1]

Riassunto
La rivoluzione globale prodotta dall'affacciarsi nel panorama internazionale della "Rete delle reti" (Internet) ha determinato mutamenti profondi in molti settori della società, veicolando un sapere condiviso garantito dall'orizzontalità delle comunicazioni, in cui i fruitori ne sono al contempo i "costruttori". Tali trasformazioni hanno coinvolto anche le logiche di governance, evidenziando la necessità di una corrispondenza fra evoluzione tecnologica ed approccio alla sicurezza, sia questa relativa alla tutela delle infrastrutture tecnologiche sulle quali poggia il Paese così come alla protezione dei cittadini. In tale prospettiva, si segnalano i più recenti interventi di ordine operativo realizzati in Italia dal Servizio Polizia Postale e delle Comunicazioni, allo scopo di fronteggiare i pericoli derivanti dai computer crimes e dai computer related crimes, quali: l'istituzione del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche Informatizzate (CNAIPIC) e del Centro Nazionale per il Contrasto della Pedofilia, l'adozione del Child Exploitation Tracking System (CETS) volto a contrastare la pedofilia on line, e l'istituzione di un Commissariato di Pubblica Sicurezza on line.

Abstract
The global revolution which arose through the coming of the Internet on the international scene has produced deep changes in many social contexts. Nowadays, it offers a common and shared knowledge thanks to horizontal ways of comunication, the users being at the same time the "producers" of it. Such a transformation also involves the field of governance, indicating the necessity to create harmony between technological growth and security policies. These regard the protection of technological infrastructures as well as the protection of all citizens. For these reasons, the Italian "Servizio Polizia Postale e delle Comunicazioni" have recently introduced some important innovations, in order to combat the risks of computer crimes and computer related crimes. They concern the institution of a "Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche Informatizzate (CNAIPIC)"; the setting up of the Child Exploitation Tracking System (CETS), in opposition to on line pedophilia; and finally the institution of a sort of "on line Police Office for Security".

1. Premessa.

"La rete delle reti", con questo appellativo si suole indicare la rete internet. Uno spazio virtuale al servizio di finalità economiche, culturali e sociali.

La veicolazione di un sapere condiviso, garantito dalla orizzontalità della comunicazione internet in cui i fruitori dell'informazione ne sono anche

[1] Dirigente Superiore della Polizia di Stato, Direttore del Servizio Polizia Postale e delle Comunicazioni.

"costruttori", ha spezzato le catene imposte dalla verticalità dello schema "emittente/ricevente" del messaggio comunicativo.

Ma il dato saliente si rileva nelle dinamiche di interazione tra gli individui. Chat, forum e *newsgroups* hanno definito luoghi di socializzazione alternativi rispetto alla piazza, l'oratorio o il cd. "muretto". E' scomparsa la prossimità, fisica e spaziale, tra gli individui che comunicano, per lasciare spazio all'intermediazione del personal computer nelle dinamiche di contatto tra gli individui. L'influenza sugli usi, costumi e stili di vita degli individui è stata decisiva.

La diffusione di modelli imprenditoriali, orientati verso piattaforme di *e-commerce*, ha inoltre contribuito ad un aumento dell'indotto ed una diminuzione dei costi di gestione per le aziende.

Ma la linea di sviluppo della Rete non si è arrestata, innalzandosi fino a coinvolgere la cabina di regia governativa attraverso l'*e-government*.

Una rivoluzione connettiva al servizio della Pubblica Amministrazione al fine di ridurre le distanze tra governo e cittadini, in virtù di una logica che vede i destinatari dei servizi pubblici quali clienti e non più meri utenti.

La differenza non è di ordine lessicale ma sostanziale. I cittadini-utenti, quali centri di interesse giuridico a cui corrispondono norme cogenti per la Pubblica Amministrazione secondo i dettami dell'imparzialità ed il buon andamento dell'azione amministrativa, sono divenuti *customer* e pertanto l'efficacia della P.A. si misura in termini di satisfaction, di gradimento nella fruizione del servizio.

In questo scenario, una concreta ed efficace logica di *governance* non può prescindere dal tenere in debita considerazione le possibili minacce ed aggressioni alla sicurezza del sistema costituito, degli interessi e dei valori sottostanti, che possono derivare da fenomeni di criminalità comune, organizzata o con finalità eversive e terroristiche.

La minaccia, la compromissione, la distruzione di un siffatto sistema tecnologico, così come la sottrazione illecita dei dati e delle informazioni dallo stesso gestiti al fine di ricavarne un immediato profitto (per quello che può essere il loro valore intrinseco) o, comunque, di utilizzarli indebitamente per altro scopo, rappresentano oggi le condotte criminali che espongono al maggior pericolo la sicurezza e la prosperità del sistema sociale nel suo complesso considerato.

Di pari passo rispetto all'evoluzione tecnologica, anche l'approccio alla tematica della sicurezza ha in effetti subito un radicale mutamento.

Il percorso seguito, al riguardo, dalla Polizia Postale e delle Comunicazioni, in virtù delle proprie specialistiche competenze in materia di prevenzione e contrasto della criminalità informatica, tende al raggiungimento di due fondamentali obiettivi:

la protezione delle "infrastrutture tecnologiche" che, sulla Rete, assumono una valenza strategica per la sicurezza e la prosperità del Paese;

la protezione degli "utenti" della Rete e dei valori che gli stessi, quotidianamente, affidano all'infrastruttura telematica ai fini della loro soddisfazione.

2. La protezione delle Infrastrutture critiche nazionali informatizzate.

I servizi essenziali per il Paese (acqua, luce gas, trasporto su strada, rotaia ed aereo) vengono oggi erogati attraverso reti telematiche che, nella loro interconnessione, trovano un formidabile strumento per garantire elevati standard di qualità nella fornitura e nell'accesso ai servizi ed effettività all'idea di uguaglianza.

Il rovescio della medaglia mostra un contesto in cui l'effetto domino è il pericolo maggiore. Un attacco informatico, di matrice criminale o terroristica, diretto a colpire un singolo nodo della rete infrastrutturale, potenzialmente è in grado di azzerare l'intero sistema.

Tale problematica è da alcuni anni al centro dell'attenzione della comunità mondiale: in differenti contesti istituzionali di collaborazione internazionale (U.E., G8, etc.), sono state adottate e vengono portate avanti iniziative di analisi ed approfondimento e si lavora per la definizione di modelli operativi condivisi.

In Italia, la legge 31 luglio 2005 nr. 155, recante "Misure urgenti per il contrasto del terrorismo internazionale", all'art. 7 bis attribuisce al Servizio Polizia Postale e delle Comunicazioni, in via esclusiva ed in virtù delle proprie specialistiche competenze, la protezione dei sistemi informatici delle infrastrutture critiche di interesse nazionale[2].

Presso il Servizio Polizia Postale e delle Comunicazioni è stato pertanto istituito il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche Informatizzate (CNAIPIC), una sorta di 113 privilegiato che attraverso collegamenti telematici esclusivi e protetti provvederà a ricevere e trasmettere informazioni e dati utili alla prevenzione e repressione delle minacce e degli attacchi informatici diretti ai sistemi delle Infrastrutture critiche nazionali.

In attesa della emissione, da parte del Ministro dell'Interno, del decreto con il quale il citato art. 7 bis dispone l'individuazione delle I.C. nazionali che potranno beneficiare dei servizi di protezione informatica resi dal CNAIPIC, il Dipartimento di pubblica sicurezza si è fatto promotore con Enti, pubblici e privati erogatori di servizi ritenuti essenziali per la Nazione, di una serie di convenzione finalizzate a stabilire protocolli di formazione per il personale e di intervento, in caso di computer incident, condivisi.

Il CNAIPIC agirà inoltre in stretto rapporto di collaborazione operativa ed interscambio informativo con gli altri organi che, a livello nazionale ed internazionale, sono coinvolti nel settore della protezione delle I.C.

I servizi di protezione informatica resi dal CNAIPIC potranno beneficiare anche di strumenti di investigativi particolarmente incisivi, tipici del settore del contrasto al terrorismo, quali le attività di indagine condotte sulla Rete con modalità

[2] L'art. 7 bis comma 1° della legge 31.07.2005 n. 155, che ha convertito con modificazioni il D.L. 27.07.2005 n. 144, recita infatti: *"Ferme restando le competenze dei Servizi informativi e di sicurezza, di cui agli artt. 4 e 6 della legge 24.10.1977 n. 801, l'organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione assicurai servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'Interno, operando mediante collegamenti*

sottocopertura e le intercettazioni di comunicazioni, anche telematiche ed informatiche, eseguite con finalità preventive[3].

3. La protezione degli utenti della Rete.

Ma il pericolo non si esaurisce con la delimitazione delle criticità tecnologiche infrastrutturali.

I recenti fatti di cronaca, legati all'incidente ferroviario avvenuto in Germania ove un treno ad alta velocità, comandato a distanza, si è schiantato su alcuni oggetti lasciati incustoditi sulle rotaie, dimostrano che i pericoli sono in agguato ed imprevedibili perché connessi ad un fattore imponderabile: l'*uomo* e la sua connaturale tendenza a violare le regole di convivenza sociale.

Dalle tradizionali forme di espressione della *criminalità*, mirate ad attingere valori intrinsecamente riconducibili alla persona, sia come individuo che come parte di una collettività (quali ad esempio l'integrità fisica o la sfera patrimoniale), si è giunti ai concetti di *computer crime* e *computer related crime*, quali fenomeni criminali in cui la tecnologia dell'informazione e della comunicazione così come il complesso di beni immateriali che la prima produce e veicola assumono, di per sé, un ruolo di primo piano nell'ambito dell'ordinamento giuridico sia come obiettivo dell'azione illecita, giuridicamente riconosciuto e tutelato, sia come strumento di consumazione del reato, al tempo stesso qualificato e qualificante rispetto a specifiche fattispecie.

Sullo sfondo di tale nuovo panorama criminale, personaggi d'antologia della criminalità e del terrorismo nostrano, quali Totò Riina, Raffaele Cutolo, Morucci e Renato Curcio, possono a ragione essere sostituiti - nell'immaginario collettivo - da intraprendenti cultori dell'informatica che, magari di giovanissima età e privi di organizzazioni strutturate alle spalle, si presentano con le medesime velleità e determinazione a delinquere dei predecessori.

E' necessario rapportarsi con l'entità della *popolazione internauta*, rappresentata dai milioni di navigatori del *world wide web*, per rendersi conto di quanto grande possa essere l'impatto criminale sul cd. "*villaggio globale*".

L'uso del pc e l'utilizzo della Rete da parte dei giovani, secondo i recenti dati Istat, è infatti cresciuto in modo esponenziale in tutte le fasce di età e circa il 70% di quattordicenni sono collegati giornalmente alla rete. Questo dato, se sotto certi aspetti ci tranquillizza e ci soddisfa per le evidenti ripercussioni positive sulla crescita sociale e culturale dei nostri ragazzi, dall'altro ci impone di innalzare la soglia di sicurezza che ad essi, così come, più in generale, alle fasce più deboli della nostra società, dobbiamo garantire durante la navigazione nella rete, affinché non siano vittime di criminali informatici.

---

telematici definiti con apposite convenzioni con i responsabili delle strutture interessate".

[3] L'art. 7 bis comma 2° della sopra citata legge 31.07.2005 n. 155 dispone, infatti, che: "*Per le finalità di cui al comma 1 e per la prevenzione e repressione delle attività di terrorismo e 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 decreto legge 18.10.2001 n. 374,convertito con modificazioni dalla legge 15.12.2001 n. 438, e quelle di cui all'art. 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28.07.1989 n. 271, anche a richiesta o in collaborazione con gli organi di polizia giudiziaria ivi indicati* ".

Pedopornografia on line, truffe via internet, azioni di hacking, diffusione di codici malevoli, clonazioni di carte di pagamento, diffusione di opere dell'ingegno in violazione del diritto d'autore, *spamming* e *phishing* sono i nuovi fenomeni criminali che minacciano la collettività, ed i valori a questa sottesi, nel suo rapporto con la Rete.

Per arginare un fenomeno delinquenziale così vasto è necessario agire attraverso una strategia altrettanto globale.

Per ciascuna delle fattispecie di reato sopra citate, e per altre ancora, la Polizia Postale e delle Comunicazioni composto da circa 2000 persone, espleta attività di prevenzione e repressione attraverso unità specializzate, distribuite sull'intero territorio nazionale (in 19 Compartimenti regionali e 77 Sezioni provinciali), e coordinate dal Servizio centrale.

Ma i nuovi interpreti principali del suddetto approccio globale sono il Centro Nazionale per il Contrasto della Pedopornografia On-line *(CNCPO)* ed il Commissariato Virtuale.

Si tratta di due unità funzionali, inserite nel Servizio Polizia Postale e delle Comunicazioni, grazie alle quali i fenomeni delinquenziali di riferimento sono costantemente monitorati al pari di un malato terminale, e "curati" attraverso specifiche attività repressive.

Il *CNCPO* è stato istituito dalla legge 6 febbraio 2006 nr. 38, recante "*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet*"[4], nella quale sono previsti diversi interventi normativi volti ad aumentare le capacità di prevenzione e contrasto dell'odiosa piaga dello sfruttamento sessuale dei minorenni. In primis la possibilità di procedere, non solo in caso di scambio ma anche di mera detenzione di materiale pedo pornografico, all'arresto facoltativo dell'indagato.

Tra le funzioni del Centro, si evidenzia anzitutto la compilazione e l'aggiornamento di una *black list,* e cioè di un elenco di indirizzi internet cui corrispondono contenuto pedopornografici, con il conseguente obbligo per gli *Internet Service Providers* di implementarlo sui rispettivi sistemi al fine di impedirne il raggiungimento da parte della propria clientela[5].

In capo agli I.S.P. grava inoltre l'obbligo, oggi, di segnalare al Centro, qualora ne vengano a

[4] L'art. 19 della sopra citata legge 06.02.2006 n. 38 prevede infatti che dopo l'articolo 14 della legge 3 agosto 1998 n. 269, recante "*Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitu'*", sia inserito, tra gli altri, l'articolo 14 *bis*, intitolato "*Centro nazionale per il contrasto della pedopornografia sulla rete INTERNET*", che recita:

"1. Presso l'organo del Ministero dell'interno di cui al comma 2 dell'articolo 14, e' istituito il Centro nazionale per il contrasto della pedopornografia sulla rete Internet, di seguito denominato "Centro", con il compito di raccogliere tutte le segnalazioni, provenienti anche dagli organi di polizia stranieri e da soggetti pubblici e privati impegnati nella lotta alla pornografia minorile, riguardanti siti che diffondono materiale concernente l'utilizzo sessuale dei minori avvalendosi della rete Internet e di altre reti di comunicazione, nonche' i gestori e gli eventuali beneficiari dei relativi pagamenti. Alle predette segnalazioni sono tenuti gli agenti e gli ufficiali di polizia giudiziaria. Ferme restando le iniziative e le determinazioni dell'autorità giudiziaria, in caso di riscontro positivo il sito segnalato, nonche' i nominativi dei gestori e dei beneficiari dei relativi pagamenti, sono inseriti in un elenco costantemente aggiornato.

2. Il Centro si avvale delle risorse umane, strumentali e finanziarie esistenti. Dall'istituzione e dal funzionamento del Centro non devono derivare nuovi o maggiori oneri a carico del bilancio dello Stato.

3. Il Centro comunica alla Presidenza del Consiglio dei ministri - Dipartimento per le pari opportunità elementi informativi e dati statistici relativi alla pedopornografia sulla rete Internet, al fine della predisposizione del Piano nazionale di contrasto e prevenzione della pedofilia e della relazione annuale di cui all'articolo 17, comma I.".

conoscenza, le imprese o i soggetti che attraverso le proprie reti di comunicazione diffondono a qualunque titolo materiale pedopornografico[6].

Di pari importanza è il rapporto di collaborazione con l'Ufficio Italiano Cambi, per l'individuazione, il tracciamento e la sospensione delle transazioni finanziarie riconducibili all'acquisto on line di materiale prodotto con lo sfruttamento sessuale dei minori[7].

L'istituzione del predetto Centro rappresenta il riconoscimento dell'incisività con la quale, nel corso di questi ultimi anni, la Polizia Postale e delle Comunicazioni ha saputo utilizzare gli strumenti normativi e tecnologici posti a sua disposizione, nello svolgere sia il quotidiano e sistematico monitoraggio della Rete, al fine di studiare le continue evoluzioni dei siti pedofili e dei loro fruitori, sia una costante attività repressiva, avvalendosi anche - in via esclusiva - di tecniche di indagine sulla Rete che prevedono modalità sottocopertura[8].

Negli ultimi 6 anni, infatti, attraverso complesse indagini svolte da investigatori sostenuti da personale specializzato in informatica, elettronica, telecomunicazioni e psicologia, sono stati identificati e denunciati 3.418 soggetti e sono stati eseguiti 164 arresti.

Sono stati rilevati in Italia e oscurati 153 siti pedopornografici, mentre altri 7.114, della stessa natura, i cui server erano collocati all'estero e irraggiungibili dalla giustizia italiana, sono stati segnalati ai rispettivi organi di polizia stranieri.

Con la collaborazione di organi di polizia stranieri si è giunti anche alla individuazione di vere e proprie reti internazionali di pedofili – una delle più grandi è stata smantellata dalla Polizia Postale di Venezia l'anno scorso con l'operazione "*Canal Grande*" (1.300 indirizzi telematici di pedofili individuati in oltre 78 Paesi, dei quali 200 in Italia).

Dal punto di vista operativo-investigativo, l'espandersi del fenomeno criminale a livello planetario ha imposto una revisione delle strategie di attacco al fenomeno stesso, facendo emergere la necessità di forme di collaborazione più strette tra i vari organi di Polizia nel mondo, e di strumenti tecnologici di indagine comuni.

In sostanza, per ottenere risultati ancora più efficaci bisognerà, nell'immediato futuro, passare da attività investigative anche eccellenti, condotte nel *web* a "*macchia di leopardo*", a strategie che, pur nel rispetto delle autonomie dei singoli Stati, investano tutto il *web* in modo coordinato e puntuale.

I presupposti principali affinché vi sia questo mutamento di strategia sono:

---

[5] Si tratta di una procedura disciplinata dall'art. 14 *quater* della legge 03.08.1998 n. 269, così come introdotto dal sopra citato art. 19 della legge 38/'06.

[6] Tale obbligo è sancito dall'art. 14 *ter* della legge 03.08.1998 n. 269, introdotto anch'esso dal sopra citato art. 19 della legge 38/'06.

[7] Le procedure in argomento sono disciplinate dall'art. 14 *quinquies* della legge 03.08.1998 n. 269, introdotto anch'esso dall'art. 19 della legge 38/'06.

[8] L'art. 14 comma 2 della legge 03.08.1998 n. 269 recita infatti: "*Nell'ambito dei compiti di polizia delle telecomunicazioni, definiti con il decreto di cui all'articolo 1, comma 15, della legge 31 luglio 1997, n. 249, l'organo del Ministero dell'interno per la sicurezza e la regolarita' dei servizi di telecomunicazione svolge, su richiesta dell'autorita' giudiziaria, motivata a pena di nullita', le attivita' occorrenti per il contrasto dei delitti di cui agli articoli 600-bis, primo comma, 600-ter, commi primo, secondo e terzo, 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 tal fine, il personale addetto puo' 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*

- che i percorsi investigativi utilizzati siano condivisi
- che lo scambio di dati e di informazioni sia continuo e in tempo reale
- ma soprattutto programmi *software* comuni che utilizzino lo stesso "*linguaggio*".

Ecco dunque il prezioso e insostituibile apporto di Microsoft.

Partendo da una delle polizie più efficienti del mondo nella lotta alla pedofilia, quella canadese, e aggregando al progetto via via tutte le altre (indonesiana, italiana, australiana, inglese, statunitense, per citarne alcune) è stato prodotto il *Child Exploitation Tracking System (CETS*), che permetterà di realizzare sul piano operativo internazionale le condizioni suddette.

In particolare, alle reti di pedofili si vuole contrapporre una rete internazionale di cyber-poliziotti che, partendo dalle esperienze nazionali, siano strettamente collegati tra di loro, che parlino la stessa lingua e che usino i più avanzati "*protocolli*" investigativi, sintesi dei vari percorsi d'indagine seguiti nei rispettivi Paesi di appartenenza.

La Microsoft ha dato concretezza al progetto fornendo il "*tessuto*" della rete e alcuni strumenti *software* in grado di tracciare i pedofili *on-line.*

Nei giorni scorsi si è concluso quindi il ciclo, durato oltre un anno, con il quale i tecnici della Microsoft, sulla base delle indicazioni fornite dagli investigatori e dai tecnici della Polizia Postale e delle Comunicazioni, hanno ridisegnato il CETS adattandolo alle esigenze operative italiane rimanendo comunque nel solco già tracciato dalla polizia canadese.

Restando sul piano delle strategie di contrasto del crimine informatico, che vede sicuramente nella pedopornografia on line la più odiosa delle sue forme di manifestazione, ma che certo nella stessa non si esaurisce, è importante sottolineare la necessità di sempre maggiori forme di collaborazione tra istituzioni e società civile.

L'istituzione del Commissariato di P.S. on line, all'interno del Servizio Polizia Postale e delle Comunicazioni, rappresenta un importante passo in avanti lungo il percorso suddetto.

Si tratta infatti di un portale *web* che offre a "cittadini internauti" una ricca serie di servizi: aree di approfondimento normativo in materia di *computer crime, chat* e *forum* interattivi per discutere di temi connessi al crimine informatico, opportunità per gli utenti del *web* di denunciare o semplicemente segnalare alla Polizia Postale e delle Comunicazioni fatti di reato di cui sono stati vittime o spettatori durante la navigazione.

Ebbene, avviandomi a concludere il mio intervento, mi preme osservare che le occasioni, come quella odierna, che ci portano a riflettere sul ruolo della Rete nella società contemporanea sono tanto più benvenute in quanto consentano a tutti di comprendere la complessità del fenomeno e le sue differenti implicazioni.

Di fronte ad una minaccia globale è necessario rispondere con altrettanta ecumenicità. E, soprattutto, in piena sinergia da parte di tutte le componenti della società dell'informazione.

Il ruolo che ad esempio rivestono, in tale contesto, gli *Internet Service Provider* è di assoluta rilevanza

al comma 1 anche per via telematica

non soltanto, come ovvio, in termini di sviluppo della Rete e dei suoi servizi, ma anche nell'ottica della loro sicurezza e prosperità a fronte delle minacce di matrice criminale e terroristica.

Gli I.S.P. sono infatti chiamati a collaborare con il *law enforcement*, entro i limiti previsti dalla legge, ai fini della stigmatizzazione dei contenuti illeciti immessi sulla Rete.

Ma, soprattutto, è chiesto loro di porre a disposizione degli inquirenti, alle condizioni di legge e nel pieno rispetto della privacy dei loro clienti, gli unici elementi informativi utili e necessari alla identificazione di chi, contro la Rete o tramite la stessa, pone in essere azioni delittuose: si tratta dei cd. *log file* e cioè dei dati *"esterni"* al traffico telematico.

La sopra citata legge 31 luglio 2005 n. 155 ha introdotto, come noto, una serie di utili correttivi al pregresso regime di conservazione dei dati di traffico[9].

E, peraltro, l'esperienza investigativa di settore dimostra che tale nuovo impianto normativo è comunque ancora perfettibile, ad esempio prevedendo il riallineamento del periodo di conservazione del traffico telematico (6 + 6 mesi) a quello del traffico telefonico (24 + 24 mesi), stante l'interdipendenza delle due diverse tipologie di comunicazione.

Assoluta rilevanza, dal punto di vista investigativo, assume inoltre l'introdotto regime di conservazione delle cd. *chiamate senza risposta*.

Gli attentati terroristici di Roma (nel 2001) e Madrid (nel 2004), i cui ordigni vennero innescati con un semplice squillo telefonico su apparati radiomobili, sono il triste esempio di quanto gli strumenti ad alto contenuto tecnologico siano oggi pienamente utilizzati dai terroristi, non soltanto per esigenze di comunicazione ed organizzazione e, conseguentemente, rappresentano un pericolo a fronte del quale non ci si può più permettere di sottostimare la valenza investigativa dei dati di traffico sulla bilancia sul cui ulteriore piatto gravano

[9] Si tratta della nuova disciplina in materia di *data retention*, introdotta dall'art. 6 della sopra citata legge 155/'05, che recita: *1. A decorrere dalla data di entrata in vigore del presente decreto e fino al 31 dicembre 2007 e' sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni, e limitatamente alle informazioni che consentono la tracciabilità degli accessi, nonche', qualora disponibili, dei servizi, debbono essere conservati fino a quella data dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore. I dati del traffico conservati oltre i limiti previsti dall'art. 132 del decreto legislativo 30 giugno 2003, n. 196, possono essere utilizzati esclusivamente per le finalità del presente decreto-legge, salvo l'esercizio dell'azione penale per i reati comunque perseguibili.*

2. All'articolo 55, comma 7, del decreto legislativo 1° agosto 2003, n. 259, le parole «al momento dell'attivazione del servizio.» sono sostituite dalle seguenti: «prima dell'attivazione del servizio, al momento della consegna o messa a disposizione della occorrente scheda elettronica (S.I.M.). Le predette imprese adottano tutte le necessarie misure affinche' venga garantita l'acquisizione dei dati anagrafici riportati su un documento di identità, nonche' del tipo, del numero e della riproduzione del documento presentato dall'acquirente, ed assicurano il corretto trattamento dei dati acquisiti.».

3. All'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni: a) al comma 1, dopo le parole «al traffico telefonico», sono inserite le parole: «, inclusi quelli concernenti le chiamate senza risposta,»; b) al comma 1, sono aggiunte in fine le parole: «, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per sei mesi»; c) al comma 2, dopo le parole: «al traffico telefonico», sono inserite le seguenti: «, inclusi quelli concernenti le chiamate senza risposta,» d) al comma 2, dopo le parole: «per ulteriori ventiquattro mesi», sono inserite le seguenti: «e quelli relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati per ulteriori sei mesi»; e) ed f) << omissis >>.

le legittime istanze di privacy e gli attuali *asset* aziendali.

Tra l'altro, l'indagine che si focalizza sui dati di traffico, telefonico o telematico, così come sulle cd. *chiamate senza risposta*, non necessariamente porta ad approfondimenti di tipo contenutistico o anagrafico: quella sul *cyber crime* è un'indagine essenzialmente i natura tecnica, asettica, focalizzata sulle mere tracce informatiche e telematiche che la condotta delittuosa dissemina sulla *Rete*; soltanto in un secondo momento, attraverso le tecniche di indagine tradizionali, si tenterà di dare un nome ed un volto all'autore del reato.