3.4 *Rapporto tra riciclaggio e finanziamento del terrorismo*

Un ulteriore aspetto da considerare è l'attenzione al riciclaggio ed ai sistemi finanziari internazionali, accesa dai tragici fatti occorsi l'11 settembre 2001 a New York.

Il primo atto ufficiale dell'amministrazione Bush nella lotta al terrorismo dopo gli eventi di settembre 2001 è rappresentato dalla dichiarazione della «guerra finanziaria» alle organizzazioni terroristiche. L'iniziativa ha reso immediatamente evidente la necessità di modificare uno dei capisaldi dei mercati finanziari internazionali: la neutralità dei capitali scambiati; principio in base al quale sui mercati i capitali tendevano a non avere più colore, né odore.

Ferme restando le differenze concettuali tra riciclaggio (definito anche *money laundering*) e finanziamento di attività illecite (definito anche *money dirtying*), l'elemento in comune tra le due figure è costituito dalla necessità, presente in entrambi i casi, di occultare la provenienza illecita del denaro o la destinazione illecita del denaro, oppure entrambe; ciò rende verosimile, oltre che probabile, che tecniche operative e canali di trasmissione possano almeno in parte coincidere.

Lo stato della lotta al finanziamento del terrorismo è ancora ai primi approcci; in questa fase, fare costante riferimento ai risultati finora raggiunti nella lotta al riciclaggio consentirebbe, da un lato, di non ripetere gli errori già commessi, dall'altro, di infondere nuova energia e soprattutto nuovi strumenti anche nella lotta al riciclaggio.

3.5 *Prospettive di adeguamento*

A tal proposito, occorre innanzitutto separare tra loro i due obiettivi principali dell'azione antiriciclaggio, cioè l'obiettivo del reperimento delle informazioni nel sistema finanziario e l'obiettivo della collaborazione degli intermediari finanziari; il che consiste, per usare termini già usati in precedenza, nella ricerca di migliori gradi di collaborazione 'passiva' ed 'attiva'.

Collaborazione «passiva»

Il primo obiettivo, dunque, è quello di consentire alle Autorità di raccogliere con efficacia informazioni finanziarie rilevanti minimizzando tempi e costi, grazie alla disponibilità dei patrimoni informativi in possesso di intermediari, imprese, professionisti; è quella che viene definita «collaborazione passiva» ed in Italia il conseguimento di questo obiettivo potrà essere facilitato dalla piena operatività dell'Anagrafe dei rapporti di conto e di deposito istituita con D.M. 4/8/2000 n. 269 in attuazione del disposto dell'art. 20, comma 4, della legge 413/1991; il decreto è stato pubblicato in G.U. 2.10.2000 n. 230 ed il 17.10.2000 è entrato in vigore il regolamento dell'anagrafe che raccoglierà i rapporti di conto e di deposito, nominativi o al portatore, in denaro o titoli, di qualunque importo e che dovrebbe essere gestita dal Tesoro.

L'anagrafe non è ancora operativa e quindi non è fruibile dai soggetti abilitati ad inoltrare la richiesta di informazioni.

In merito, appare opportuno fare qualche precisazione che gioverà nella comprensione dell'effettiva portata dei benefici che il sistema di contrasto al riciclaggio potrà trarre dall'anagrafe dei rapporti di conto e di deposito, contribuendo inoltre a ridimensionare i dubbi avanzati in ordine alle deroghe al segreto bancario recate dalla norma.

Infatti, le informazioni che sarà possibile richiedere attraverso la consultazione dell'Anagrafe dei conti concernono i conti correnti, i depositi (sia nominativi, sia al portatore, in denaro o titoli) ed ogni altro rapporto continuativo rientrante nell'esercizio dell'attività istituzionale dell'intermediario relativo all'amministrazione e alla gestione dell'attività patrimoniale dell'impresa; concernono, inoltre, anche i rapporti cointestati o relativamente ai quali la persona indagata agisce in nome e per conto di altri soggetti o ne può disporre.

Le richieste potranno essere volte a conoscere se, nell'archivio dei soggetti interrogati, esistono rapporti riconducibili alla persona oggetto dell'accertamento e, in caso positivo, l'identificazione compiuta dell'intermediario ove il rapporto è intrattenuto nonché gli estremi del rapporto di conto o di deposito.

I risultati ottenibili con l'entrata in funzione del nuovo strumento operativo sarebbero sicuramente apprezzabili in termini di abbattimento dei tempi di esecuzione delle indagini bancarie.

Come risulta anche dal rapporto presentato nel luglio 2004 dal CNEL – Osservatorio socioeconomico sulla criminalità - *«Il dispositivo antiriciclaggio: bilanci e prospettive»*, tutti gli organismi istituzionali ed associativi consultati dall'Osservatorio (Banca d'Italia, UIC, ABI, Organismi giudiziari ed investigativi impiegati nello specifico settore) condividono la necessità di una celere attuazione della normativa istitutiva dell'anagrafe dei conti e dei depositi, sottolineando il significativo dispendio di risorse materiale ed umane conseguente alla prassi delle notifiche 'a pioggia', da un lato, nonché gli enormi ritardi sofferti dalle indagini dovuti al diradarsi dei tempi di risposta degli intermediari alle richieste di notizie circa la sussistenza di rapporti con determinati soggetti, dall'altro. In merito allo specifico punto, pur non essendo stati prodotti dati statistici, è stato ritenuto che le indagini presso gli intermediari bancari e finanziari scontano ritardi nell'ordine di mesi a causa delle difficoltà ad individuare l'esatta allocazione dei rapporti sui quali concentrare l'investigazione.

Invero, uno dei problemi venuti in evidenza nel notevole lasso di tempo trascorso dall'emanazione della normativa che per prima ha previsto l'Anagrafe in questione è connesso alla prevista costituzione di un'unità operativa presso il Ministero del tesoro avente il compito di ricevere le richieste dagli Organi abilitati e diramarle agli intermediari; il problema è sinora consistito nel numero esatto dei destinatari finali del messaggio e nel mantenimento delle garanzie di riservatezza delle notizie.

Altro problema in più sedi evidenziato è relativo ai costi di realizzazione e di gestione della stessa Anagrafe, presumibilmente proporzionali al numero di intermediari che entrano a far parte della rete di dati.

Il dato che oggettivamente va rilevato è rappresentato dagli sprechi e dai ritardi scontati per effetto del ritardo, che si traducono inevitabilmente in una perdita di efficienza e di efficacia del sistema di prevenzione del riciclaggio; obiettivi cui è necessario tendere con fermezza e con la consapevolezza dei benefici che ne conseguirebbero per la sicurezza dell'intero sistema economico.

Una celere attuazione pratica della previsione normativa, infatti, avrebbe come primo effetto la velocizzazione della procedura di richiesta di informazioni da parte delle Autorità titolari dei relativi poteri di accertamenti bancari (sarà, infatti, possibile per il verificatore individuare con precisione i rapporti di conto e di deposito, evitando richieste dispersive alle varie direzioni centrali degli istituti di credito).

Tuttavia, è opportuno sottolineare, per diradare ogni residuo dubbio sulla reale portata dello strumento, che per entrare nel contenuto dei singoli rapporti e, quindi, verificare i singoli movimenti sarà necessario procedere con gli ordinari mezzi investigativi poiché i dati contenuti nell'«anagrafe» saranno relativi solo agli estremi dei rapporti, alle date di accensione e chiusura, ai codici fiscali dei titolari, dei cointestatari e di chiunque altro possa disporne. Inoltre, la precisione della previsione normativa, che fa riferimento ai conti, ai depositi e ad ogni altro rapporto duraturo, fa sì che non saranno rinvenibili nell'anagrafe tutte le operazioni che non siano state poste in essere da un soggetto in presenza di un rapporto contrattuale duraturo con l'intermediario (ad esempio, le richieste di assegni circolari o le richieste di bonifici effettuate per contanti). La normativa, inoltre, esclude espressamente i conti transitori, le cassette di sicurezza ed i depositi chiusi.

Collaborazione «attiva»

L'altro obiettivo è quello della «collaborazione attiva» degli operatori del mercato finanziario.

Come visto in precedenza, se i mercati bancari e finanziari non assumessero la legalità come valore assoluto cui tendere costantemente, la collaborazione attiva finirebbe per comportare costi che potrebbero apparire all'operatore ancora maggiori dei benefici attesi.

Ora, premessa l'opportunità, di ordine generale, di giungere all'individuazione di regole condivise dagli stessi operatori, è necessario che il sistema sia indotto ad adottare condotte di collaborazione «attiva» anche attraverso la predisposizione di norme sanzionatorie, che, nell'analisi costi-benefici, pesino sulla scelta dell'operatore in ordine al grado di collaborazione da assicurare.

In merito a tale aspetto, se si considerano analiticamente i pericoli di instabilità e di generale compromissione in cui il sistema incorre quando – con comportamenti non necessariamente collusivi ma anche semplicemente negligenti – si rende permeabile ad operazioni di riciclaggio, se ne può dedurre l'inclusione di tutte le disposizioni emanate a difesa del sistema finanziario dal rischio di riciclaggio nel più ampio novero delle norme sulla sana e prudente gestione, che costituisce uno dei perni delle

norme di vigilanza di settore raccordate nel testo unico delle leggi bancarie (d.lgs. n.385/1993).

Proprio il TULB, inoltre, prevede penetranti poteri di controllo dell'attività di vigilanza in ordine, tra le altre finalità, anche alla sana e prudente gestione dei soggetti vigilati [195]; l'inosservanza di tali disposizioni può anche condurre, da parte degli Organi di vigilanza, all'adozione di provvedimenti molto incisivi, quali l'amministrazione controllata e la liquidazione coatta amministrativa (art. 70 e seguenti del TULB).

L'introduzione di efficaci forme di responsabilità [196] a carico di intermediari che non si siano dotati di adeguate strutture di controllo interno potrebbe determinare negli stessi operatori l'adozione di protocolli preventivi idonei a minimizzare il pericolo di perpetrazione del reato attraverso le proprie strutture, allontanando in tal modo il rischio di sanzioni. Questa soluzione è stata già adottata in altri ordinamenti (ad esempio nell'ordinamento francese: art. 324-9 C. pèn.) ed è attualmente in discussione in altri Paesi, come quello elvetico.

Non c'è dubbio che le sanzioni appena viste rappresenterebbero per gli intermediari il «costo» dell'inosservanza delle disposizioni nella specifica materia; tale costo lieviterebbe ulteriormente qualora si prevedessero, in aggiunta all'irrogazione delle suddette sanzioni, adeguate forme di pubblicità che andrebbero ad incidere su uno dei valori su cui si regge il sistema degli intermediari bancari, finanziari ed assicurativi: la reputazione [197].

Un sistema di regole così costruito è certamente in grado di incidere in modo positivo su ciò che è ritenuto importante dagli intermediari, potendo addirittura determinarli a creare dall'interno una struttura di incentivi nelle singole mansioni indirizzata verso comportamenti di collaborazione attiva nell'impegno contro il riciclaggio.

I centri *off-shore*

In materia di lotta al finanziamento al terrorismo, l'OECD ha fornito quattro indicazioni di cui i singoli Stati sovrani dovranno tenere conto all'atto di predisporre la normativa di prevenzione e di contrasto al fenomeno.

La prima affermazione è la constatazione che la rete mondiale bancaria e finanziaria è vulnerabile ai rischi di finanziamento al terrorismo.

La seconda affermazione è che tale rischio equivale al rischio da riciclaggio di capitali illeciti.

La terza considerazione è che nel mercato mondiale possono verificarsi questi rischi in quanto esistono delle falle, dei «buchi neri», rappresentati dai centri *off-shore;*

---

[195] I dati sono tratti dalla nota del Comandante Generale della Guardia di Finanza pervenuta alla Commissione il 3 agosto 2003.

[196] Relazione annuale della Commissione – luglio 2003 – pag. 247.

[197] È evidente, peraltro, che il rischio di perdita della riservatezza diverrebbe inconsistente in presenza di norme che adeguatamente delimitino l'ambito di circolazione delle informazioni messe a disposizione degli Organi abilitati.

In ultimo, si afferma l'equivalenza di tali centri tra loro, in quanto catalizzatori del rischio di finanziamento al terrorismo ma anche del rischio di dannosità fiscale, poiché si ritiene che le falle della rete bancaria e finanziaria mondiale (appunto, i centri *off-shore*) facilitino il finanziamento al terrorismo, il riciclaggio dei capitali illeciti e la concorrenza fiscale sleale tra Stati sovrani.

In un volume di recente pubblicazione è stata condotta l'analisi delle precedenti affermazioni, riportate come estrema sintesi dei principi enunciati dalla produzione documentale internazionale in materia. L'analisi riconosce che oggettivamente l'industria bancaria e finanziaria mondiale è fisiologicamente vulnerabile ai rischi di finanziamento al terrorismo e di riciclaggio, a causa delle differenze di distribuzione delle informazioni tra i vari soggetti (ricorre la «asimmetria informativa»).

I Paesi *off-shore* finanziari [198] mostrano caratteristiche strutturali, sia economiche sia istituzionali molto omogenee, poiché sono Paesi e territori non particolarmente ricchi, poveri di risorse naturali, con forte dipendenza dal reddito prodotto dai servizi bancari e finanziari, normalmente privi di particolari problemi legati al rischio terrorismo ed al rischio criminalità organizzata.

Ciò che appare evidente a fattor comune per il rischio riciclaggio e per il rischio di finanziamento al terrorismo è l'assoluta necessità che il dibattito internazionale tenga conto del rischio causato dai centri *off-shore*, poiché la presenza di falle nel sistema compromette seriamente l'esito degli sforzi profusi a livello nazionale dai singoli Stati per contrastare condotte criminose sempre più frequentemente caratterizzate dalla transnazionalità.

L'alto beneficio che i Paesi *off-shore* si attendono dal mantenimento di una regolamentazione lassista aumenta la difficoltà a rendere conveniente per tali Paesi, a livello generalizzato, l'adozione di legislazioni idonee a prevenire i rischi di inquinamento del sistema; ciò deve impegnare la comunità internazionale ad affrontare caso per caso la realtà dei singoli Paesi alla ricerca delle soluzioni di volta in volta ritenute più appropriate.

Lo strumento cui sinora si è più frequentemente fatto ricorso in sede internazionale per il contrasto al finanziamento al terrorismo è costituito dalla *blacklist*, consistente nell'individuazione dei Paesi non cooperativi ai quali si minacciano sanzioni in assenza di credibili presidi volti ad arginare il rischio di agevolare il finanziamento al terrorismo ed il riciclaggio di capitali di matrice illecita (lo strumento della *blacklist*, alla quale collegare previsioni sanzionatorie, è stato utilizzato anche dall'Italia per individuare i Paesi *off-shore* fiscali).

---

[198] Un sistema di sanzioni più pregnanti, peraltro, non sarebbe nuovo nel nostro ordinamento. La Banca d'Italia, infatti, già detiene penetranti poteri di controllo – in ordine alla verifica di una sana e prudente gestione – previsti dall'art. 5 T.U.L.B. (D.Lgs. n.385/1993); detti poteri possono condurre all'amministrazione straordinaria o alla liquidazione coatta amministrativa, al divieto di intraprendere nuove operazioni o alla chiusura di succursali.

La presenza dei centri *off-shore*, la globalizzazione dei mercati e la transnazionalità dei reati perpetrati dalla criminalità organizzata richiedono una risposta organica ed articolata sul piano internazionale, prima ancora che su quello nazionale, alla ricerca di una volontà comune tesa a predisporre mezzi di controllo, di tipo politico e di tipo giuridico, che consentano di superare il sistema che si è venuto a creare, in cui i modelli di controllo e le regole sono in notevole ritardo rispetto alla rapidità di movimento dei flussi finanziari.

È innegabile, infatti, che l'abolizione di frontiere per persone, merci e capitali si accompagna ancora oggi all'esistenza di frontiere ben salde per le istituzioni e per le regole giudiziarie e di polizia; l'avvio di processi significativi di armonizzazione e di omogeneizzazione merita attenta considerazione e nuovi impulsi da parte di ogni Paese.

In proposito, è opportuno fare un riferimento al progetto di ricerca denominato *«EUROSHORE – La protezione del mercato finanziario europeo dallo sfruttamento dei Paesi offshore ed altri centri finanziari da parte della criminalità organizzata»* ultimato nel corso del 2000 [199].

Il progetto di ricerca, finanziato nell'ambito del «Programma Falcone» dalla Commissione europea, è stato realizzato da Transcrime, Centro interdipartimentale di ricerca sulla criminalità transnazionale dell'Università di Trento (prof. E. Savona), in collaborazione con il Certi – Università Bocconi di Milano (prof. V. Uckmar) – e con la Facoltà di Giurisprudenza dell'Università Erasmus di Rotterdam in Olanda (prof. H. De-Doelder).

Mirando all'obiettivo di contribuire allo sviluppo delle azioni e degli strumenti finalizzati alla prevenzione della criminalità organizzata nel territorio dell'UE, il progetto si è basato sul concetto di prevenzione dello sviluppo delle organizzazioni criminali, attuata riducendo le opportunità dei loro affari attraverso un sistema di de-regolazione o di ri-regolazione di quei 'mercati' dove si incontrano domanda ed offerta di servizi illeciti. Tale concezione è naturalmente in linea con le strategie elaborate a livello internazionale contro la criminalità organizzata, che individuano nei Paesi off-shore un problema serio da porre ai primi posti dell'agenda delle varie istituzioni internazionali.

La ricerca ha raggruppato i 48 Paesi analizzati in tre gruppi di «centri finanziari», in base al loro livello di prossimità agli Stati membri dell'UE (prossimità politica, geografica, economica); ai tre gruppi è stato affiancato un quarto gruppo omogeneo costituito dai paesi UE (Gruppo 0).

I Gruppi sono:

Gruppo 1: *Centri finanziari e giurisdizioni offshore europei*. Sono Paesi che hanno contatti di tipo geografico, economico o politico con l'UE: Andorra, gli *Overseas Territories* (che comprendono Anguilla, Ber-

---

[199] Indebita percezione e truffa in erogazioni pubbliche, frode informatica, corruzione, concussione, falsità in monete ed ora anche delitti aventi finalità di terrorismo e di eversione dell'ordine democratico per effetto della legge n. 7/2003 di ratifica della Convenzione di New York del 9 dicembre 1999, in materia di repressione del finanziamento del terrorismo.

muda, Gibilterra, isole Vergini Britanniche, isole Cayman, isole Turks e Caicos), i *Caribbean Territories* del regno d'Olanda (che comprendono Aruba ed Antille Olandesi), Cipro, i *French West Indies Departments*, le isole del Canale (che comprendono Jersey e Guernsey), l'isola di Man, Malta, Liechtenstein, Principato di Monaco, San Marino, Svizzera.

Gruppo 2: *Economie in transizione*, cioè giurisdizioni appartenenti all'*ex* blocco sovietico o situate nella regione balcanica: Albania, Bulgaria, Moldavia, Estonia, Lettonia e Lituania, Repubblica Ceca, Polonia, Romania, Repubblica Slovacca, Slovenia, Ucraina, Ungheria.

Gruppo 3: *Giurisdizioni offshore esterne all'UE*. Sono giurisdizioni che non hanno alcun tipo di connessione con l'UE: Bahamas, Barbados, Giamaica e Portorico, Isole Cook, Hong Kong e Macao (Cina), Malesia, Nauru, Niue, Seychelles, Singapore, Vanuatu, etc.

I risultati della ricerca risultano sintetizzati nei due grafici che seguono.

Il grafico 1 rappresenta la deviazione dei quattro gruppi di Paesi dagli *standard* di integrità per i diversi settori di regolazione considerati: maggiore è questa distanza (quando la deviazione si allontana da 0 e si avvicina a 1), peggiore è il livello di integrità di quel settore di regolazione per il relativo gruppo di Paesi.

Il grafico 2, invece, rappresenta la distanza dei tre gruppi di Paesi per i diversi settori di regolazione dai corrispondenti *standard* di integrità dei Paesi dell'UE: più la deviazione si allontana dal valore 0 e si avvicina a 1, maggiore è la distanza dei livelli di integrità di questi Paesi da quelli dell'UE. Pertanto a maggiore deviazione corrisponde un maggiore rischio di sfruttamento di questi Paesi per fini criminali e, di conseguenza, un maggiore rischio di inquinamento per il sistema finanziario europeo.

Grafico 1. Deviazione di ciascun Gruppo dagli standard di integrità in ciascun settore di regolazione.

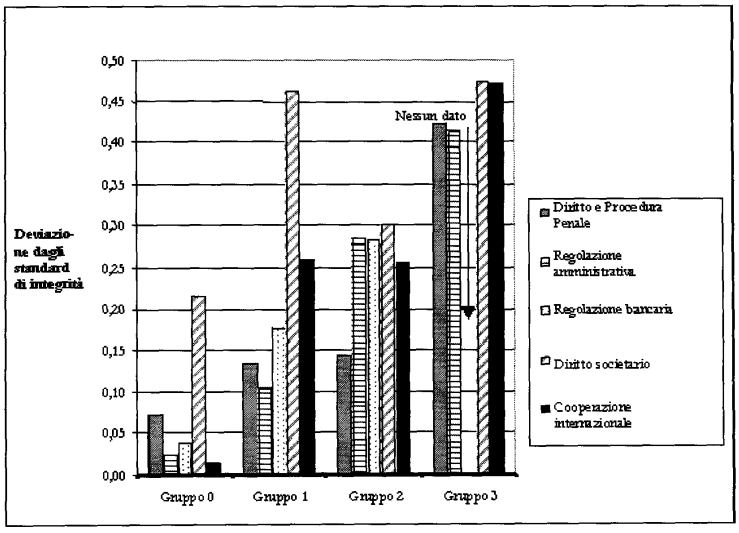
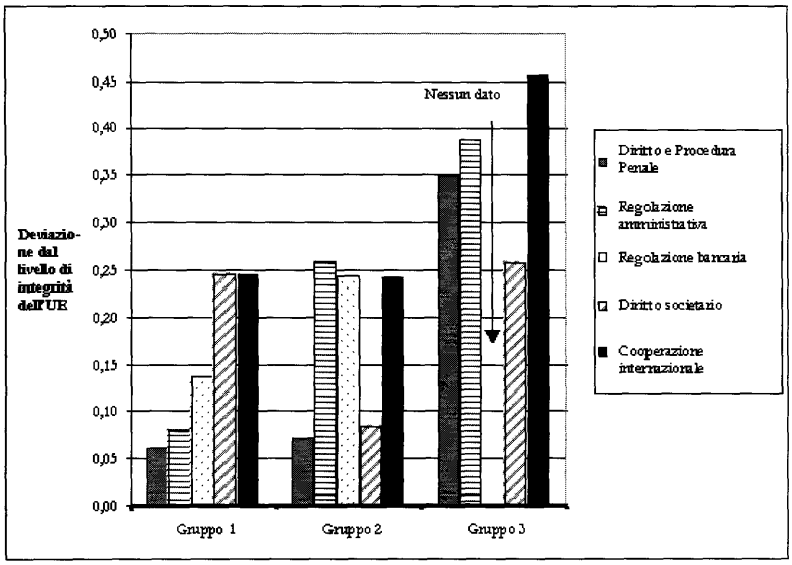


Grafico 2. Deviazione dei Gruppi 1, 2 e 3 dal livello di integrità dell'UE



Anche dalle informazioni, necessariamente sommarie, che provengono dai grafici, è chiaro che se un impegno è richiesto nei confronti delle giurisdizioni dei Paesi *offshore*, opportuno sembra anche un monito ai Paesi più vicini all'area UE o addirittura appartenenti ad essa, rispetto ai quali in alcuni settori si riscontrano differenze considerevoli tra le quali si annidano i rischi di infiltrazione dei capitali di origine o di destinazione illecita.

La lotta al riciclaggio dei capitali illeciti, così come quella al finanziamento al terrorismo, dunque, potrà presumibilmente accrescere le proprie speranze di successo innanzitutto con una effettiva presa di coscienza collettiva del rischio di destabilizzazione rappresentato dall'immissione nel circuito economico lecito di capitali di matrice o di destinazione illecita.

Tale presa di coscienza deve passare attraverso un'analisi che evidenzi tutti gli aspetti di rischio che possono derivare dal mantenimento di una situazione pari a quella attuale. Il Fondo Monetario Internazionale, con una stima peraltro non aggiornata a quest'anno, valuta che i capitali che vengono riciclati ogni anno attraverso il sistema finanziario internazionale si collocano tra 500 e 1.500 miliardi di dollari all'anno, pari a circa il 5% del prodotto monetario.

Come noto, dopo l'11 settembre 2001, gli Stati Uniti hanno emanato una legge più severa (si tratta del *Patriot Act*[200]) per contrastare il fenomeno e hanno intensificato l'azione di cooperazione internazionale.

---

[200] Gli artt. 51 e seguenti del titolo III del TULB prevedono, ad esempio, in materia di vigilanza sulle banche, l'obbligo per gli intermediari di trasmettere alla Banca d'Italia i bilanci; o, ancora, poteri di vigilanza ispettiva in capo alla Banca d'Italia.

A livello nazionale, l'approntamento di regole idonee ad abbassare i rischi finora evidenziati potrà fruttuosamente puntare su ciò che più caratterizza i mercati bancari e finanziari: la distribuzione delle informazioni.

Solo se le informazioni circoleranno, se saranno livellate le differenze nella distribuzione delle informazioni tra Autorità – inquirenti ed investigative – ed operatori di mercati si abbasserà la vulnerabilità dei mercati bancari e finanziari al rischio di riciclaggio.

Unitamente all'incentivazione della cd. «collaborazione passiva» dovrà essere attuata l'incentivazione della «collaborazione attiva», anche mediante la predisposizione di regole condivise che adeguino il sistema sanzionatorio in modo da rendere 'conveniente' per gli intermediari il rispetto delle prescrizioni normative poste a tutela dei sistemi finanziari nazionale ed internazionale.

3.6 *Conclusioni*

È oramai noto l'effetto distorsivo creato dall'immissione di grandi masse di denaro liquido di provenienza illecita nel circuito economico lecito. Il principio della libera concorrenza economica, infatti, risulta fortemente turbato da imprenditori in grado di finanziare la propria attività senza fare ricorso al credito bancario; a ciò si aggiungano i rischi derivanti dal deposito di ingenti masse di capitali illeciti presso la stessa banca sì da determinare, in caso di improvviso ritiro, rischi di crisi dell'istituto di credito che, in tal modo, diviene potenzialmente esposto ad azioni ricattatorie.

Analoghe considerazioni valgono in relazione al fenomeno dell'usura ed alle conseguenti pericolose ricadute sul tessuto produttivo e sull'ordine pubblico poiché le organizzazioni criminali giungono, attraverso la concessione di prestiti a tassi usurari, al controllo ed all'acquisizione di strutture imprenditoriali lecite da utilizzare, in seguito, per il riciclaggio dei proventi dei traffici illeciti mediante la costituzione di altre linee di finanziamento illimitato, alternative ai canali bancari, e così via; fino al rischio che non residui più alcuno spazio operativo per gli imprenditori onesti [201].

È, altresì, noto a tutti i livelli che i riciclatori operano di solito in contesti transnazionali, seguendo schemi operativi resi estremamente vari anche grazie all'utilizzo delle tecnologie informatiche (per cui si trovano spesso combinati tra loro il trasferimento elettronico dei fondi, l'utilizzazione di società di copertura o l'uso di fatture per operazioni inesistenti, l'acquisizione di garanzie e via procedendo).

Le organizzazioni criminali, inoltre, ricorrono ad istituzioni finanziarie non bancarie per l'illecita esportazione di valuta, facendo confluire i fondi da riciclare nei sistemi finanziari di Paesi diversi da quelli in cui

---

[201] Come visto in precedenza, in dottrina si è prospettata la possibilità che la tecnica adottabile per giungere a tale estensione possa consistere nella previsione di forme di responsabilità analoghe alla responsabilità amministrativa di persone giuridiche prevista per i casi di corruzione dal D.Lgs. 231/2001.

sono stati commessi i reati presupposto e che non dispongono di adeguate legislazioni antiriciclaggio nonché utilizzando società di copertura normalmente collocate in Paesi *off-shore* o 'non cooperativi'.

La difficoltà ad operare per perseguire i responsabili di tali illecite condotte e la presa di coscienza da parte dei singoli Stati sovrani della necessità di contrastare in modo globale i crimini economico-finanziari, al fine di limitare l'espansione geografica delle conseguenze negative indotte dalla loro commissione, hanno condotto alle varie iniziative in ambito internazionale [202] sulla spinta delle quali viaggia l'adeguamento degli ordinamenti nazionali.

I sistemi bancari e finanziari sono sistemi caratterizzati da «asimmetria» nella distribuzione delle informazioni tra i soggetti che partecipano al mercato; le informazioni, infatti, catalizzate dagli operatori bancari che hanno sviluppato un alto grado specialistico nella loro trattazione, non sono acquisibili né facilmente, né a basso costo.

Ciò rende estremamente interessanti per le organizzazioni criminali i sistemi bancari e finanziari, poiché in mercati con tali caratteristiche è basso il rischio che l'operazione di riciclaggio emerga con rilievo investigativo.

Se la caratteristica di tali mercati è la distribuzione asimmetrica delle informazioni, probabilmente la soluzione per ottenere un sistema veramente efficiente è da ricercare proprio in tale direzione: un livellamento nella distribuzione delle informazioni che consenta alle Autorità un più facile accesso alle informazioni in possesso degli operatori.

Il versante di intervento non può, però, essere solo questo poiché è oramai chiaro che solo una partecipazione convinta degli operatori possa rendere efficace il sistema. I fattori che intervengono nell'analisi costi-benefici che ciascun operatore effettua per valutare il grado di accettabilità della normativa antiriciclaggio sono, da un lato, la perdita dell'assetto di riservatezza che caratterizza tradizionalmente gli appartenenti al sistema

---

[202] Senza alcun intento di risoluzione della questione, che meriterebbe attenta ed approfondita discussione parlamentare, si ricorda che l'art. 6, comma 3, della legge 50/1994 - recante «Modifiche alla disciplina concernente la repressione del contrabbando dei tabacchi lavorati» – prevedeva, a carico degli acquirenti di sigarette di contrabbando, sanzioni accessorie che consistevano proprio in forme di pubblicità della sanzione principale.

Il testo dell'art. 6 della legge 18 gennaio 1994, n. 50 è il seguente:

Ai soggetti sorpresi ad acquistare sigarette ed altri tabacchi lavorati esteri di contrabbando, oltre alle sanzioni penali previste dal citato testo unico approvato con decreto del Presidente della Repubblica n. 43 del 1973, o da altre leggi speciali, è irrogata anche una sanzione amministrativa nella misura fissa di lire centomila. In deroga alla legge 7 fennaio 1929, n. 4, e successive modificazioni, ed alla legge 24 novembre 1981, n. 689, non è ammessa alcuna forma di pagamento in misura ridotta.

Le violazioni di cui al comma 1 sono accertate e le relative sanzioni sono riscosse nei modi di cui agli articoli 13 e seguenti della citata legge n. 689 del 1981. L'Ufficio competente a ricevere il rapporto di cui all'art. 17 e ad emettere l'ordinanza-ingiunzione di pagamento di cui all'art. 18 della medesima legge n. 689 del 1981 è individuato negli Ispettorati Compartimentali dell'Amministrazione Autonoma dei Monopoli di Stato.

L'Ispettorato Compartimentale di cui al comma 2 dispone inoltre la pubblicazione della sanzione comminata a spese del soggetto sanzionato, su uno o più giornali. *(omissis).*

bancario e, dall'altro, gli oggettivi costi che l'operatore stesso deve sostenere per mantenere una struttura che gestisca e trasmetta le informazioni.

Se però si considera che il sistema bancario si fonda anche su un altro valore, quello della reputazione dell'operatore, ecco che il sistema di soluzioni da adottare per rendere il sistema più efficace potrebbe essere orientato in altre direzioni: ad esempio, l'introduzione di ipotesi di responsabilità amministrativa per le persone giuridiche (del tipo di quelle già introdotte per fatti di corruzione) articolato non solo sulle sanzioni pecuniarie ma su sanzioni più gravi, mutuabili dallo stesso sistema di norme in materia di intermediazione bancaria e finanziaria e veicolabili all'interno del sistema di prevenzione del riciclaggio attraverso un'estensione del concetto di sana e prudente gestione.

Tali sanzioni, corredate da un adeguato sistema di pubblicità delle sanzioni irrogate, appaiono idonee a divenire efficace remora per gli operatori bancari e finanziari, ma anche per gli altri soggetti obbligati al rispetto delle norme in materia di identificazione, registrazione e segnalazione delle operazioni; essi, infatti, sarebbero indotti a dotarsi di adeguati sistemi di controllo interno al fine di minimizzare i rischi che il sistema venga usato per fini di riciclaggio, allontanando, così, il pericolo di sanzioni.

La necessità e l'opportunità delle modifiche proposte poggia sulla considerazione, condivisa da opinioni autorevoli, che anche l'attuale sistema di repressione penale del riciclaggio risulta privo di effettività, ove per effettività si intenda sia il tasso complessivo di osservanza della norma (da parte dei destinatari e da parte di chi è destinato all'implementazione del sistema di prevenzione), sia il raggiungimento dello scopo tutelato dalle norme.

Infatti, pur a fronte del crescente volume d'affari dell'economia criminale e dunque presumibilmente anche delle relative attività di riciclaggio, l'esame dei repertori giurisprudenziali e delle statistiche giudiziarie incontra casi veramente rari in cui è stato ritenuto applicabile l'art. 648-*bis* c.p.; ancora meno risultano quelli in cui è stato applicato l'art. 648-*ter* c.p.

I pochi casi che si incontrano, peraltro, sono spesso relativi ad ipotesi delittuose-presupposto, rispetto alle quali la fattispecie del riciclaggio si presenta caratterizzata addirittura da ipereffettività; talvolta, infatti, i reati presupposto che hanno dato luogo a contestazioni per riciclaggio (punito, si ricorda, con la reclusione da quattro a dodici anni) è stato il furto di autovetture alle quali erano state sostituite le targhe o manomesso il numero di telaio [203].

---

[203] Talvolta si trovano elencazioni in cui gli *off-shore* finanziari sono distinti dagli *off-shore* fiscali; in tal caso, si intendono con i primi i Paesi con una legislazione accondiscendente che aumenta i rischi di finanziamento al terrorismo e di riciclaggio; si intendono con il termine *off-shore* fiscali quei Paesi con regimi fiscali agevolati. Peraltro, non sempre un *off-shore* fiscale è anche un Paese *off-shore* finanziario.

L'indifferibile necessità di un'azione adeguatrice del sistema trova ulteriore conforto nel documento approvato dalla VI Commissione permanente – Finanze e Tesoro – del Senato, «*Indagine conoscitiva sui possibili fenomeni di riciclaggio connessi all'imminente circolazione dell'euro nel nostro Paese.*

Nella seduta del 18 dicembre 2001, la citata Commissione ha espresso la convinzione che le esigenze di contrasto e di definitiva sconfitta delle grandi organizzazioni criminali, nazionali ed internazionali impongano un'indicazione di priorità che metta in primo piano il bisogno di legalità, sicurezza e trasparenza, rispetto a considerazioni, pur meritevoli di attenzione, di ordine garantistico.

In conclusione va citato il documento, approvato dalla Commissione nella seduta plenaria del 23 marzo 2004, con cui viene rassegnato un contributo al Parlamento in occasione della discussione della legge di ratifica della Convenzione ONU sui crimini transnazionali.

In tale documento, in ordine all'art. 7 della Convenzione, che ribadisce l'obbligo per gli Stati-parte di istituire e mantenere un sistema di prevenzione del riciclaggio che soddisfi le prioritarie esigenze di identificazione dei clienti, di registrazione delle operazioni e di segnalazione delle operazioni sospette, la Commissione rileva l'impegno del nostro Paese dotato, fin dal 1991 (D.L. n. 143), di una disciplina adeguata ed efficace che, prevedendo gli obblighi di identificazione della clientela, di registrazione delle operazioni e di segnalazioni di movimentazioni sospette, ha anticipato i capisaldi delle misure antiriciclaggio individuati proprio dalla Convenzione in esame (art. 7 paragrafo 1 lett. a).

La Commissione ha, altresì, ribadito la necessità di dare piena attuazione alla normativa di settore, con particolare riferimento all'operatività dell'Anagrafe dei rapporti di conto e di deposito alla cui istituzione – prevista dall'art. 20, comma 4, della legge n. 413 del 1991 – si è dato luogo mediante decreto interministeriale n. 269 del 2000 ma che, tuttavia, difetta dell'ulteriore normativa di attuazione.

Ha ritenuto, inoltre, malgrado la legge n. 350 del 2001 non abbia inciso sulla disciplina antiriciclaggio, che debba compiersi uno sforzo ulteriore, al fine di rendere le attività economiche assolutamente trasparenti e identificabili nei soggetti interessati (soprattutto, sotto il profilo sostanziale) nonché rintracciabili i percorsi dei flussi di denaro.

Recenti scandali finanziari, ancorché allo stato non risultino coinvolgimenti di soggetti riferibili ad organizzazioni criminali, hanno dimostrato l'esistenza di punti critici del sistema, di cui è naturale ritenere possano avvalersi anche le organizzazioni criminali.

Viene, quindi, ritenuto indispensabile un esame complessivo della normativa vigente, allo scopo di migliorarne l'efficacia, oltre che l'effettività applicativa nonché di eliminarne profili contrari ai principi sanciti in sede internazionale e comunitaria.

4.0 La dimensione metaterritoriale del crimine informatico

Negli ultimi anni si è diffuso il concetto di «guerra asimmetrica» [204] – un termine che oggi è familiare anche ai non specialisti – pur dovendosi rilevare che molti osservatori si sono fermati ad un primo livello ermeneutico di tale concetto, quello connesso al contesto bellico/terroristico e specificatamente alle differenti strategie fra le operazioni degli eserciti tecnologicamente avanzati e gli attacchi di realtà minoritarie, spesso sfuggenti, prive di strutture istituzionali e di potenza militare *strictu sensu* intesa.

Al contrario la «guerra asimmetrica» può divenire una semiotica adatta a descrivere anche contesti di aggressione agli Stati da parte del crimine organizzato.

La scena dell'attacco alle *Twin Towers* dell'11 settembre 2001 è bene impressa nell'inconscio collettivo; in quel contesto l'arma di distruzione di massa era l'uomo suicida, che utilizzava a fini militari oggetti che *ictu oculi* non suggerirebbero un tale uso; oggi però quella lettura merita un ampliamento, che nasce dalla presa di coscienza della vulnerabilità intrinseca di alcuni elementi che sono ormai imprescindibili nel nostro sistema di vita.

Nelle analisi di scenario più accreditate, quali quelle degli specialisti della *Rand Corporation*, John Arquilla e David Ronfeldt [205], emerge da diversi anni l'idea che il confronto attuale contro il terrorismo e il crimine organizzato si stia spostando dal terreno reale della vita quotidiana a quello virtuale delle reti telematiche: nasce il concetto di *Netwar*, la «Guerra in Rete», all'interno del quale si preconizza un progressivo impiego delle risorse informatiche da parte dei gruppi criminali organizzati transnazionali.

Ancora più precisamente, l'aspetto di rischio transnazionale del crimine, già ampiamente messo in luce nella precedente Relazione della Commissione, troverebbe una forte amplificazione proprio nell'espandersi in un «metaterritorio» senza frontiere e definiti vincoli giuridici quale è attualmente il cosiddetto *cyberspace*, vale a dire il mondo dell'informazione supportato dalle reti telematiche, che trova in Internet la sua massima espressione di pervasività sociale.

---

[204] Il progetto è stato predisposto nell'agosto del 1998 su iniziativa del Ministero della Giustizia italiano e come seguito alla Raccomandazione n. 30 del Piano d'Azione dell'UE contro la criminalità organizzata dell'aprile 1997, secondo la quale gli Stati Membri «*devono analizzare quali siano le possibili modalità di intervento e adottare le difese che sono necessarie contro lo sfruttamento, da parte della criminalità organizzata, dei centri finanziari e delle giurisdizioni* offshore*, soprattutto se questi siano situati in località geografiche sottoposte alla giurisdizione dei Paesi Membri. Per quanto riguarda, invece, i centri finanziari e le giurisdizioni* offshore *situate al di fuori della giurisdizione dei Paesi Membri, il Consiglio deve adottare una politica comune, coerente con quella adottata dagli Stati Membri al loro interno, per impedire che questi centri siano, d'ora innanzi, sfruttati dalle organizzazioni criminali che operano sul territorio comunitario*».

[205] Significa: *Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*.

Qualsiasi osservatore è in grado di constatare che tutte le funzioni vitali del nostro mondo globalizzato e complesso, dai sistemi militari a quelli economico finanziari e al mondo dell'informazione, sono da tempo traslate in uno spazio virtuale, il *cyberspace*, dal quale esse non possono fattualmente più essere richiamate, pena la caduta verticale di tutto l'equilibrio sociale e geopolitico del pianeta.

Se si vuole trovare ampia riprova del precedente assunto e fondare una corretta valutazione del rischio basta scorrere l'analisi [206] del *trend* di crescita dei siti WEB nel mondo nel decennio 1995-2005 dalla quale si rileva una curva in fortissima crescita, salvo una lieve flessione tra il 2001 e il 2003: il numero di *host* nel dicembre 1994 era di 5.846.000 mentre nello stesso mese del 2004 si tocca la cifra di 317.646.000. Nei primi mesi del 2005 sono registrati quasi 65 milioni di siti dei quali 35 milioni esplicano un'attività rilevante. In Italia la crescita dei siti WEB e delle attività *ondine* [207] sembra crescere più velocemente della media mondiale e si attesta, secondo i dati 2002/2004, fra le prime cinque o sei posizioni del pianeta. Significativa appare la crescita degli utenti internet cinesi, che si avviano a divenire entro la fine del 2005 la prima *cyber*-potenza mondiale nonostante l'esistenza di un forte controllo politico che limita il libero accesso alle informazioni. Vi è anche da dire che gran parte del mondo è ancora fattualmente isolato da Internet e che il Nord America e l'Europa realizzano l'80% delle attività in rete, con fortissima concentrazione delle transazioni negli Stati Uniti; tuttavia, seppure con grandi ritardi, si registra un *trend* di crescita anche in Africa.

L'espansione verticale del commercio elettronico è un esempio classico di questo processo di translazione sostanziale dei processi produttivi ma non è l'unico; anche le metodologie criminali ne subiscono un profondo influsso.

Non a caso in tema di riciclaggio si parla ormai di *tracce digitali* delle operazioni illecite, quando sino a pochi anni or sono veniva invocato il controllo della «pista di carta» lasciata dai passaggi del denaro.

---

[206] Riciclaggio ed usura costituiscono, insieme, gli strumenti attraverso i quali le associazioni criminali raggiungono il controllo economico del territorio; le due fattispecie si intersecano tra loro, ciascuna costituendo di volta in volta mezzo, strumento o fine dell'altro reato. Infatti, l'organizzazione criminale ricicla i proventi illeciti anche attraverso l'erogazione di credito usurario; attraverso il credito d'usura la stessa associazione acquisisce il controllo di imprese in difficoltà che successivamente possono essere utilizzate per il riciclaggio dei proventi illeciti; le liquidità ripulite, inoltre, possono a loro volta essere reinvestite nell'usura, fino a creare un circuito perverso che rappresenta una grave minaccia per l'economia.

[207] Si ricordano:

– la *Dichiarazione di Principi del Comitato di Basilea*, emanata nel dicembre del 1988;

– la *Convenzione delle Nazioni Unite contro il traffico illecito di sostanze stupefacenti e psicotrope*, firmata a Vienna il 20 dicembre 1988;

– le *40 raccomandazioni del Gruppo di Azione Finanziaria Internazionale (G.A.F.I.)*;

– la *Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato*, firmata a Strasburgo l'8 novembre 1990;

– il *Gruppo Egmont*.

Un altro paradigma del mondo di Internet è dato dalla sua complessità architetturale che accentua i fattori di criticità specie nel settore della sicurezza.

Il comune dato esperienziale dell'utilizzatore di *personal computer* dimostra una diuturna crescita verticale della minaccia anche spicciola in termini di diffusione di virus informatici e di altri oggetti *software* ostili – il cosiddetto *malfare* – capaci non solo di creare indisponibilità di servizio nei sistemi posseduti ma anche di violare la *privacy* e la riservatezza delle informazioni possedute, come dimostra l'aumento costante dell'area di *business* legata al mercato di strumenti *hardware* e *software* di difesa dalle intrusioni [208].

Vi è anche da sottolineare che talune tendenze egemoniche che caratterizzano la diffusione di soluzioni software nel mercato informatico facilitano non soltanto la creazione del *malware* ma anche la sua rapida diffusione sulle reti planetarie: così come la differenziazione biologica tra le specie costituisce un baluardo insostituibile nei confronti degli agenti patogeni, anche una razionale e pianificata diversità di ambienti operativi informatici potrebbe aumentare la resilienza dei sistemi rispetto ad un paradigma troppo uniforme.

La sensibilità per tali problemi è percepibile anche negli atti normativi comunitari, quali la direttiva 2000/31/CE (Direttiva sul Commercio Elettronico) e la direttiva 2002/58/CE (Direttiva relativa alla vita privata e alle comunicazioni elettroniche). Questa ultima direttiva fa parte del «pacchetto Telecom» che dal 24 aprile 2002 disciplina il settore delle comunicazioni elettroniche. Con Regolamento 460/2004 in data 10 marzo 2004 il Parlamento ed il Consiglio hanno approvato l'istituzione dell'Agenzia Europea per la sicurezza delle reti e dell'informazione.

In ambito normativo nazionale il recepimento delle direttive europee si è attuato con l'entrata in vigore del Codice in materia di protezione dei dati personali, avvenuta il 1º gennaio 2004.

Tale interesse tecnico-giuridico appare assai adeguato alla minaccia, in considerazione del fatto che un ulteriore aspetto della moderna *Netwar* consiste nella possibilità di sferrare attività offensive da parte di piccoli ed elusivi gruppi reticolari di specialisti – facilmente reclutabili in paesi caratterizzati da problematiche di reddito individuale ma anche da presenza di cospicue risorse umane formate in ambito tecnologico (ad esempio la Russia o l'India) – senza necessità di dover «schierare le proprie truppe», ovverosia di dover costituire una logistica visibile ed investigativamente tracciabile dell'attività criminale.

Nella riunione di marzo 2005 in sede ONU [209] degli esperti mondiali sul sequestro di persona, cui ha partecipato come esperto italiano un con-

---

[208] Tra le altre si fa riferimento a Cass, sez. II, 28.3.2003, n.18577; Cass., sez. II, 12.12.2003, n.47684; Cass., sez.I, 14.5.1997; Tribunale Asti, 13.6.2001; Tribunale Piacenza, 11.12.2000; Appello Cagliari, 18.9.1996.

[209] Qiao Liang e Wang Xiangsui, *Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione*, Libreria Editrice Goriziana, 2001.

sulente della Commissione, i delegati dell'India e della Cina hanno presentato casi di studio sul *trend* attuale del fenomeno, evidenziando l'uso massivo delle comunicazioni internet nella fase di negoziazione del riscatto in una dimensione transnazionale che ha consentito ai gruppi criminali estremo orientali di gestire l'attività criminosa in Canada nei confronti dei parenti delle vittime.

Emerge da questi studi una nuova tipologia di coordinamento delle attività criminali che non richiede più la relazione diretta dei soggetti inseriti nel gruppo criminale e sostituisce ad essa la relazione virtuale del mondo informatico, modificando i caratteri sostanziali del *modus operandi* delittuoso e rendendo assai più complessa l'attività investigativa.

4.1 *Criminalità organizzata informatica*

Il Rapporto sulla Sicurezza del Ministero dell'Interno per l'anno 2005 dedica uno specifico paragrafo alla criminalità informatica attualizzando attraverso i dati operativi il rischio che ho prima tratteggiato:

«Il mondo delle comunicazioni e le sue applicazioni, in particolare internet, hanno raggiunto, negli ultimissimi anni, un elevato livello di tecnologia ed una diffusione d'uso notevole, con un conseguente ed allarmante incremento dei reati commessi attraverso l'utilizzazione o in danno di questi mezzi informatici, che ormai presidiano ogni attività della vita civile del cittadino. Si assiste, infatti, ad un moltiplicarsi di comportamenti criminali nella rete Internet, che integrano le diverse fattispecie di reati, dalle frodi telematiche e telefoniche, alle violazioni del diritto alla privacy *e del diritto d'autore, alla pornografia minorile, all'aggressione dei sistemi informatici di aziende ed imprese, con danni economici incalcolabili, sia per il semplice cittadino, utente della rete, sia degli utenti qualificati pubblici e privati, per i quali la rete internet è diventata strumento imprescindibile di lavoro. Il fronte delle aggressioni informatiche e delle truffe su Internet sembra essere il contesto criminologico emergente sul piano del c.d.* high tech crime. *Per quanto riguarda le intrusioni informatiche da parte dei c.d.* hackers *vi è stato, negli ultimi dodici mesi, un aumento dei casi denunciati da parte di aziende colpite, con un conseguente incremento delle attività investigative svolte da parte della Polizia Postale e delle Comunicazioni che hanno portato alla puntale identificazione e al deferimento all'Autorità giudiziaria dei responsabili delle aggressioni criminali subite dalle imprese. Il dato significativo rispetto al passato è che si comincia a manifestare una maggiore propensione delle aziende alla denuncia dei crimini informatici subiti*[210]*, mettendo quindi gli inquirenti in condizione di operare con efficacia anche in tale settore particolarmente importante per la vita economica del Paese. Non vi è dubbio infatti che il patrimonio informativo delle aziende e delle imprese italiane costituisce un obiettivo remunerativo per i criminali informatici. La peculiarità*

---

[210] *Preparing for Conflict in the Information Age,* Rand Corporation 1997.