

tenuto contribuiti da enti pubblici in ragione di tali fittizi indebitamenti e avevano indebitamente ammortato beni strumentali inesistenti⁴⁷.

Usura: stante la diffusione del fenomeno, esso rappresenta uno dei migliori canali di riciclaggio, anche atteso il pesante ritorno di investimento.

Società fittizie: il sistema prevede la realizzazione di strutture operative apparentemente differenziate, ma, in realtà, destinate a coprire il vero assetto societario unitario, che si muovono integrando sinergicamente diversi settori di *business* contigui, quali l'intermediazione finanziaria, la vendita di beni o materiali e la gestione immobiliare. L'obiettivo è quello di supportare reciprocamente gli sforzi operativi, in modo che la connessione delle attività, spesso ottenuta con pressioni mediate sul circuito dell'utenza, possa da un lato incanalare un flusso di riciclaggio e, dall'altro, attivare un ciclo virtuoso a cascata, che renda possibile il recupero legale del denaro illecito investito con ampie plusvalenze.

Circuito bancario: una buona descrizione delle numerose metodiche di riciclaggio, effettuate usando il circuito bancario, è reperibile in un'opera del Prefetto Nicolò Pollari, attuale Direttore del S.I.S.Mi.⁴⁸. L'utilizzo di questo canale è fondato principalmente attraverso il sistema classico delle compensazioni valutarie, ivi comprendendo anche il rilascio di fideiussioni da conti esteri - alimentati da proventi illeciti - nei confronti di società nazionali, che, in tale guisa, ottengono mutui da enti di credito per operazioni imprenditoriali. In tale modo, si avvia un'impresa nata su capitale illecito, che, però, si atteggia come rispettosa delle regole del mercato, creando, se il suo lavoro sarà positivo, opportune *plusvalenze* all'originale flusso di riciclaggio. Esistono forti dubbi che un tale sistema possa essere preventivamente rilevato dal sistema di vigilanza, che non prende in considerazione le garanzie, ma solo le somme trassate.

Una diversa metodica utilizza l'investimento in titoli all'estero, avvalendosi della liberalizzazione valutaria e dell'abbattimento delle frontiere in ambito comunitario.

Circuiti finanziari alternativi e abusivi: il decreto legislativo nr. 385/1993 vieta la raccolta del risparmio, sia sotto forma di depositi, sia sotto ogni altra forma, da parte di soggetti diversi dalle banche. Analogο divieto esiste per le forme di abusiva attività finanziaria, espletata tramite operazioni di concessione di finanziamenti, prestazione di servizi di pagamento ed intermediazione nei cambi, espletate da soggetti diversi da quelli autorizzati nell'elenco previsto dall'art. 106 del Testo Unico Bancario. In effetti, specialmente nell'Asia meridionale e orientale, esiste una forma di credito «alternativo», che si è ramificato in occidente ed è noto con il nome di «*Hawalla*»⁴⁹: in tale circuito, il trasferimento di denaro avviene

⁴⁷ *Rassegna dell'Arma dei Carabinieri* - Quaderni n. 2 del 2000.

⁴⁸ *Tecnica delle inchieste patrimoniali per la lotta alla criminalità*, Firenze 1996.

⁴⁹ Il termine è una traslitterazione di una parola urdu, il cui significato è riferibile al concetto di «*fiducia*».

utilizzando banchieri abusivi, installati con un lavoro di copertura presso gioiellerie, cambiavalute o agenzie di spedizioni, che operano senza alcuna documentazione. Depositando una somma presso un «*banchiere hawalla*» in Asia, il cliente riceverà una ricevuta⁵⁰, che costituisce elemento fiduciario sufficiente per ottenere il pagamento del corrispettivo in altro paese straniero, ove operi un corrispondente della stessa catena.

Uno studio di particolare interesse, che conferma e riepiloga i meccanismi illustrati in questa relazione, è stato redatto dal Dr. Giovanni Guarnaccia per conto dell'Ufficio Italiano Cambi. In data 13 agosto 2001, il Servizio Centrale Operativo della Polizia di Stato, nell'ambito delle indagini di cui all'operazione TATIANA (Proc. Pen. 54431/99), trasmetteva tale studio alla D.D.A di Bologna, allo scopo di porre le basi di un paradigma interpretativo degli investimenti russi illegali all'estero ai fini di riciclaggio.

2.4 I «paradisi» fiscali e bancari

Questo argomento merita una trattazione a parte, non potendosi sottovalutare l'attrazione che le attività di riciclaggio possono subire per quei paesi, nei quali l'ordinamento giuridico prevede forti facilitazioni, fiscali e bancarie, anche a favore di soggetti non residenti.

A parte la valutazione della reale efficacia dei servizi offerti, che potrebbero consistere anche in una mera truffa ai danni di sprovveduti, il sito Internet della *O.P.M Corporation*⁵¹, con asserita sede a Panama e sede commerciale a Santo Domingo nella Repubblica Dominicana, offre, a scopo promozionale, una sintesi concettuale estremamente precisa di questo particolare contesto: «Offshore: significa letteralmente fuori dalle acque territoriali o, in caso di una operazione finanziaria, realizzarla fuori dal Paese di residenza (operazione extraterritoriale). Quindi, perché andare Offshore? Semplicemente per proteggere i suoi capitali.

E perché ho bisogno di proteggermi?

L'industria *offshore* è piccola e misteriosa, nonostante secondo le ultime stime oltre il 60 per cento dei capitali mondiali vengono gestiti attraverso questa industria.

Per diverse ragioni, il mercato *offshore* è stato additato come illegale e pericoloso. Molti pensano erroneamente che è un mercato riservato solo alle grandi fortune. Questa è la opinione di persone disinformate o che hanno interesse a far credere che è un mercato pericoloso per non perdere i propri clienti. [...] Un **PARADISO FISCALE** è un paese straniero che possiede una serie di caratteristiche peculiari, la più importante delle quali è che applica una tassazione minima o zero sui capitali esteri. [...] O.P.M. CORPORATION, fondata nel 1992, è una delle società *leader* nei servizi legali *offshore*. Attraverso la nostra sede nella Repubblica Dominicana e la nostra base a Panama, offriamo i migliori pacchetti *offshore*, che compren-

⁵⁰ Detta «Chit», che può assumere le forme più anonime e svariate.

⁵¹ <http://www.paradisifiscali.org>.

dono: costituzione di società anonime; amministrazione di attività commerciali; registro di nomi e patenti; residenze estere, ecc. [...]. Attraverso società anonime e fondazioni d'interesse privato proteggiamo il vostro capitale e organizziamo la vostra contabilità in modo tale da ridurre il carico fiscale. I paradisi fiscali sono una delle principali chiavi per gli investitori e solo pochi professionisti li utilizzano propriamente.

Solamente operando da un territorio *offshore* si riesce a limitare la responsabilità degli azionisti riducendo nello stesso tempo il carico fiscale.

10 BUONE RAGIONI PER APRIRE UNA SOCIETÀ ANONIMA IN UN PARADISO FISCALE:

1. per gestire anonimamente una società italiana o di un qualsiasi altro paese;
2. per proteggere i vostri beni in Italia o all'Estero;
3. per proteggersi economicamente da un doloroso divorzio;
4. per eludere il pagamento dell'imposta sul trasferimento dei beni immobili;
5. per evitare sequestri giudiziari;
6. per rifatturare merci e servizi;
7. per ridurre il carico fiscale;
8. per evitare le tasse di successione e garantire un miglior futuro alla vostra famiglia;
9. per investire all'Estero;
10. per crearsi un'alternativa economica nel più completo anonimato».

È evidente che significativa parte di queste dieci *buone ragioni* risulta estremamente appetibile anche per le attività di riciclaggio, in quanto il concetto di *paradiso fiscale* è strettamente collegato non alla bellezza del paesaggio ma all'ordinamento giuridico vigente: si osserva che, nonostante gli oggettivi progressi determinati dal lavoro internazionale per limitare queste aree di rischio, nella maggioranza dei casi gli aspetti spiccatamente garantistici del sistema bancario – essenzialmente riferibili alla tutela del segreto contro la penetrazione investigativa – vanno di pari passo con una forte permissività del settore fiscale, specie per i non residenti.

Le ragioni di tali atteggiamenti vanno ricercate nel fatto che tali «*paradisi*» sono dislocati in nazioni, che, perduto il supporto finanziario di Stati più potenti, dei quali erano state colonie⁵², avendo un ridotto territorio e scarse capacità produttive⁵³ oppure essendo andate soggette a trasformazioni rapide e non ben governate⁵⁴, si trovano nella reale necessità

⁵² È il caso delle Antille, delle Isole Cayman, delle Seichelles, di Barbados e di Hong Kong.

⁵³ Come il Liechtenstein e il Lussemburgo.

⁵⁴ Come l'Ucraina.

di trovare alternative nell'affluenza di grandi capitali stranieri, provenienti da soggetti fisici o giuridici, che desiderano sfuggire ai controlli e alle pressioni fiscali di normative più rigorose in patria.

Un ulteriore elemento che viene valutato è la stabilità politica degli Stati in questione, affinché sia garantita nel tempo la linea politica che sottende le facilitazioni bancarie e fiscali⁵⁵.

Il G.A.F.I., nel 1989, emanò un documento contenente le famose «*Quaranta Raccomandazioni*», cui i paesi aderenti debbono obbligatoriamente aderire, che costituiscono la base di standardizzazione su cui modulare la legislazione in materia di riciclaggio e la corrispondente cooperazione internazionale.

L'elemento fondamentale di queste Raccomandazioni, che negli anni sono andate incontro a revisioni ed ottimizzazioni, è il principio che obbliga gli Stati aderenti a prevedere nella propria legislazione il delitto di riciclaggio, consentendo attività investigative di tipo bancario e coinvolgendo le istituzioni bancarie e finanziarie nell'accertamento delle operazioni sospette.

Tale figura di reato non doveva, infatti, limitarsi solo ai proventi del narcotraffico e doveva prevedere la confisca dei beni correlati all'attività di riciclaggio.

I principi guida del documento⁵⁶ stabiliscono, oltre la previsione normativa del delitto di riciclaggio:

- l'obbligo per le istituzioni finanziarie di identificare i clienti, di registrare la documentazione e di segnalare le operazioni valutarie più rilevanti. Questo comporta l'eliminazione dei conti anonimi o con nomi fittizi, il monitoraggio dei *wire transfer* internazionali, la diminuzione dell'uso del contante nei pagamenti e la conservazione dei dati per cinque anni;

- l'obbligo per le istituzioni finanziarie di segnalare le operazioni sospette senza il rischio di violare vincoli di segretezza. È prevista la creazione di una banca dati centralizzata per accogliere le segnalazioni sospette provenienti dal circuito bancario;

- la comunicazione da parte delle autorità di vigilanza delle operazioni sospette alle autorità inquirenti e la collaborazione in indagini sul riciclaggio;

- la collaborazione internazionale in campo giudiziario e/o amministrativo, creando statistiche anche a fine di indagine, agevolando lo scambio informativo su soggetti sospetti, semplificando le procedure per l'estradizione e promuovendo la cooperazione nell'esercizio dell'azione penale.

Queste linee guida sono state ampiamente recepite nella Direttiva Comunitaria 91/308/CEE del 10 giugno 1991, relativa alla prevenzione del-

⁵⁵ Non a caso i siti internet dei servizi *offshore* contengono spesso puntuali analisi della situazione politica dei paesi, ove si consiglia di installare conti ed imprese.

⁵⁶ Pubblicato nell'aprile del 1990 e reperibile sul sito <http://www.fatf-gafi.org>.

l'uso del sistema bancario per il riciclaggio dei proventi di attività illecite. Importante appare la norma che estende tali prescrizioni anche ad attività professionali e categorie diverse dagli enti creditizi e finanziari, che possano essere inquinate da fenomeni di riciclaggio.

Sulla base delle Raccomandazioni emanate il 22 giugno 2000, il GAFI pubblicò un rapporto sui c.d. *paradisi finanziari* e sui *paesi non collaborativi*, individuando 25 criteri pratici per identificare le metodiche che si oppongono alla cooperazione internazionale in materia di riciclaggio: per tale via, vennero indicati quindici paesi⁵⁷ non collaborativi, sollecitandoli ad adottare le necessarie misure, onde evitare sanzioni.

Venne anche stilata una *lista grigia* di altri 14 paesi⁵⁸, il cui comportamento non si ispirava alla dovuta chiarezza normativa ed operativa in termini di riciclaggio.

La lista nera è stata modificata nei rapporti degli anni successivi, avendo molti paesi ottemperato alle raccomandazioni del GAFI ed essendo invece emersa la negativa situazione di altri, tra i quali spicca l'emersione dell'Egitto, della Nigeria e dell'Ucraina.

Il *Financial Action Task Force on Money Laundering (FATF)* del GAFI, nella sua ultima *review* annuale del 20 giugno 2003, dichiara paesi o territori non cooperativi i seguenti:

- Isole Cook;
- Egitto;
- Guatemala;
- Indonesia;
- Myanmar;
- Nauru;
- Nigeria;
- Filippine;
- Ucraina.

Nel documento si dà atto, tra altri, alla Nigeria, alle Filippine e all'Ucraina di aver compiuto taluni passi in avanti, ma non ancora sufficienti per esprimere un parere positivo.

L'*Indonesia* e *Myanmar* sembrano non aver compiuto adeguati progressi sino al giugno 2002, mentre *Nauru* continua ad essere soggetta a contromisure.

Le *Bahamas*, *Dominica*, *Grenada*, *l'Ungheria*, *Israele*, *il Libano*, *le Isole Marshall*, *Niue*, *la Russia* e *St.Kitts e Nevis* sono ancora sottoposte a processi di monitoraggio.

Nell'anno 2002-2003, in ordine ai gravi fatti terroristici avvenuti nel settembre del 2001, il FATF ha operato una rivisitazione delle *Quaranta*

⁵⁷ Bahamas, Isole Cayman, Isole Cook, Domenica, Israele, Libano, Liechtestein, Isole Marshall, Nauru, Niue, Panama, Filippine, Russia, St.Kitts e Nevis, St.Vincent e le Grenadines.

⁵⁸ Antigua e Barbuda, Belize, Bermuda, Isole Vergini Britanniche, Cipro, Gibilterra, Guersney, Isola di Man, Jersey, Malta, Mauritius, Monaco, Samoa, St. Lucia.

Raccomandazioni, sulla base dell'esperienza conseguita e, in modo speciale, per aver notato il crescente utilizzo di tecniche sofisticate, quali il crescente utilizzo di professionisti in supporto alle reti criminose che operano il riciclaggio. La combinazione delle *Quaranta Raccomandazioni* con le *Otto Speciali Raccomandazioni* sul finanziamento dei gruppi terroristici hanno dato origine ad un quadro omnicomprensivo e coerente per la lotta al riciclaggio e per combattere il finanziamento delle cellule terroristiche⁵⁹.

Il FATF ha, inoltre, ammesso come nuovi membri il Sud Africa e la Federazione Russa.

2.5 *Cyber-laundering*

Attesa la complessità del contesto finanziario attuale, le relative movimentazioni si muovono interamente attraverso le reti telematiche e ogni singola operazione è riconducibile ad un ridotto set di dati in transito tra gli elaboratori degli istituti di credito interessati: la «*pista di carta*» è divenuta una «*pista di bit*».

Per questa ed analoghe considerazioni, è crescente l'attenzione investigativa verso il mondo telematico, come esplicitato nelle puntuali riflessioni del Dipartimento di P.S. nella già citata Relazione Annuale⁶⁰.

La frammentazione degli scambi e la stessa tecnologia delle reti, pure a fronte degli opportuni strumenti di monitoraggio, facilita quella *stratificazione* complessa di operazioni, atta ad allontanare la fonte delle risorse dalla loro reale destinazione; stratificazione che abbiamo visto essere la natura profonda della meccanica dei fenomeni di riciclaggio.

Nell'esame della criminalità organizzata nigeriana, è stato già affrontato il problema delle società di *Money Transfer*, che, in alternativa al cir-

⁵⁹ Questo nuovo *framework* operativo è detto *AML/CFT* (*Anti Money Laundering/Combating Terrorist Financing*).

⁶⁰ «*Nell'ambito del complesso tema del riciclaggio, meritano un particolare approfondimento quegli aspetti che direttamente o indirettamente hanno un'incidenza rilevante nella perpetrazione di tale reato e che ne costituiscono oggi "le nuove frontiere". Il riferimento è alle transazioni telematiche, favorite dalla diffusione della rete internet che assicura un sistema di comunicazione globale impostato secondo un approccio multimediale (trasmissione in tempo reale di immagini, testi e suoni) e si distingue per il suo rivoluzionario grado di diffusione mondiale e per le difficili possibilità di controllo sui contenuti dei messaggi. Internet si è rivelato un formidabile strumento di promozione del commercio e di circolazione della moneta elettronica, in grado di assicurare livelli di anonimato, convertibilità, trasferibilità, economicità ed efficacia senza precedenti. A questo si aggiunga che nella rete trovano spazio operatori dislocati in paesi off shore in grado di offrire servizi bancari e finanziari del tutto simili ai modelli classici dell'intermediazione (cyberlaundering). Tali servizi vengono proposti in forma riservata e anonima ed a costi estremamente competitivi cosicché, pur essendo principalmente rivolti a soggetti dediti ad attività strumentali all'evasione fiscale, ben si prestano a finalità di riciclaggio dei proventi illeciti. Giova, infine, sottolineare che Internet offre l'accesso a siti dove è possibile reperire informazioni su sofisticate tecniche di criptazione dei dati e delle comunicazioni; su come ottenere "passaporti" e seconde cittadinanze assieme a conti bancari anonimi, carte di pagamento elettronico e di credito anonime, carte d'identità, nonché su come costituire società anonime off shore».*

cuito bancario, supportano transazioni finanziarie in tempo reale in tutto il mondo: la rete dei subagenti e dei submandatari costituisce, per i motivi che sono stati analizzati, un vincolo e un possibile ostacolo alla rilevazione delle operazioni sospette⁶¹.

L'ammontare complessivo dei trasferimenti effettuati in Italia attraverso il sistema del *Money Transfer* per l'anno 2001 è stato stimato in 1 miliardo e mezzo di euro.

Con tale cifra il nostro Paese è diventato il secondo mercato, per volume di affari, dopo gli Stati Uniti d'America e, valutate le differenze sociali ed economiche tra i due paesi, si può sicuramente ritenere che siamo di fronte ad un fenomeno di notevole interesse, da analizzare sotto il profilo della sicurezza.

Si è già accennato al fattore abilitante della rapidità dei trasferimenti, ma si deve anche sottolineare la facile fruizione del servizio e la diffusione capillare sul territorio sia in Italia che all'estero, servendo così in modo ottimale quella fascia di utenza, che, per vari motivi – taluni fattuali, altri ricadenti nell'illecito – non hanno accesso al sistema finanziario tradizionale, come accade agli immigrati clandestini.

In terzo luogo è emerso che talune falle del settore hanno reso talvolta possibile l'utilizzo del circuito da parte delle organizzazioni criminali o terroristiche, tanto da indurre il GAFI ad emettere alcune *Raccomandazioni Speciali* sul contrasto finanziario al terrorismo, per quanto attiene i sistemi di trasferimento di fondi alternativi a quello bancario.

Si è già detto sulla strutturazione in Italia delle Agenzie di *Money Transfer*, dipendenti da due grandi multinazionali, ma operanti attraverso una fitta e spesso scarsamente controllata rete di subagenti, dislocati in *Phone Center*, supermercati⁶², ecc.

Come si è precisato, è nella responsabilità dell'agente l'effettuazione delle verifiche antiriciclaggio previste dalla legge italiana, mentre la sede operativa del circuito internazionale, effettuate a sua volta verifiche atte ad evitare che le controparti del trasferimento siano soggetti a rischio inseriti in specifiche *black list*, approva la transazione e fornisce il codice univoco di autenticazione della stessa.

In ragione di questo assetto, gli agenti del *Money Transfer* operano come intermediari finanziari, cui è posto l'obbligo di iscrizione nel particolare elenco previsto dal Testo Unico Bancario e sono sottoposti alla normativa della legislazione antiriciclaggio (obbligo di identificazione della clientela, di registrazione delle transazioni e di segnalazione delle operazioni sospette). Al contrario, il ritiro del denaro all'estero è soggetto

⁶¹ Come, per ultimo, evidenziato dai Magistrati della DNA e della D.D.A. di Catanzaro nell'audizione del 24 giugno 2003, in riferimento a un sensibile flusso di transazioni tra la Calabria e la Germania.

⁶² Questa dislocazione nei supermercati ha attratto l'attenzione della D.D.A. di Catanzaro, come si evince dall'audizione del 24 giugno 2003, a fronte delle infiltrazioni mafiose esistenti in tale settore di commercio.

alle leggi in uso nello specifico paese e, quindi, si può assistere a notevoli variazioni di trattamento.

Appare importante sottolineare che le transazioni di questo circuito sono contraddistinte da un esclusivo impiego di denaro contante: poiché è sempre vero l'adagio *pecunia non olet*, il sistema in oggetto diminuisce la tracciabilità delle somme trassate e riduce sensibilmente l'efficacia degli strumenti di controllo.

Come derivato dei servizi Internet a disposizione di tutti, l'*home banking* ha eliminato la necessità di ricorrere al tradizionale sportello bancario, ponendo operatori non bancari nelle condizioni di immettere denaro nel circuito creditizio, di effettuare pagamenti, di movimentare capitali: a fronte di buone prestazioni nella sicurezza delle reti, questi servizi si vanno espandendo nel gradimento dell'utenza, facendo sí che ogni computer casalingo o aziendale si possa facilmente trasformare in una postazione bancaria.

Già nel rapporto del 1999, il FATF segnalava la preoccupazione delle forze dell'ordine dei paesi membri, in ordine alle accresciute potenzialità di riciclaggio connesse agli utilizzi delle tecnologie telematiche.

In particolare, tra i rischi sono stati individuati:

- incapacità ad identificare ed autenticare i soggetti che utilizzano questi sistemi;
- il livello di trasparenza della transazione;
- la mancanza o l'inadeguatezza degli strumenti di *auditing* in materia di memorizzazione ed analisi delle transazioni sospette;
- il normale utilizzo nelle sessioni di strumenti di crittografia – sempre più evoluti a fini di sicurezza contro l'*hacking* – che rendono impossibile la comprensione degli eventuali traffici internet intercettati nel corso delle indagini.

Come noto, dal 1999 ad oggi, l'uso dell'*home banking* si è diffuso ed evoluto, anche in ragione dell'estrema comodità di accesso da parte dell'utenza, non più necessitata a ricorrere all'operatore di sportello.

Tutti i sistemi richiedono che le operazioni *on-line* siano legate a conti bancari già esistenti presso l'istituto di credito dei cui servizi ci si avvale, originando un continuo flusso di informazioni inerenti le attività dei conti movimentati.

È bene però sottolineare che, per la natura stessa del mezzo telematico, non c'è alcuna possibilità di verificare l'identità del soggetto reale, che esegue transazioni tramite Internet, una volta che il conto è stato attivato e viene acceduto con la corretta procedura di sicurezza.

Questo, unitamente alla possibilità di attivare i conti direttamente su via telefonico/telematica, induce una relativa facilità⁶³ di reperire prestatori di basso profilo – addirittura inconsapevoli – i quali, dopo aver con-

⁶³ Negli ultimi tempi, onde frenare questo fenomeno, le modalità di apertura di conto sulle c.d. «*banche virtuali*» richiedono una maggiore interattività dell'utente rispetto al passato, circostanza, questa, che limita almeno le condotte più spudorate.

segnato i dati di accesso al sistema informatico, nulla più sapranno degli esiti futuri e poco potranno riferire, anche a seguito di eventuale identificazione in un contesto investigativo.

È altrettanto evidente il fatto che, se la realtà finanziaria *on-line* si trova in un'area di elevato livello di segreto bancario e/o richiede ridotte (o addirittura assenti) prove di identità per l'apertura di un conto, l'eventuale riciclatore può muovere capitali direttamente dal proprio *personal computer* in rete⁶⁴, con una rapidità assolutamente sconosciuta rispetto al passato, diversificando le transazioni su istituti bancari remoti: dopo il secondo «salto» oculato, la possibilità di ricostruire il flusso della transazione diviene molto ardua e onerosa in termini temporali.

A titolo di mero esempio, la *Micheloud & Co.*, con uffici in Svizzera a Geneva, Sion e Lausanne, permette di aprire un conto *Internet banking*⁶⁵, che offre una totale possibilità di gestione di tutte le operazioni, compresi i bonifici internazionali: il sito internet dedica una significativa parte al segreto bancario svizzero, illustrandone la nota impermeabilità.

Per chi, invece, volesse percorrere frontiere ancora più avanzate, la *E-Gold Corporate* permette di attivare celermente su Internet conti basati su una *valuta elettronica*, fondata sull'oro e su altri metalli preziosi, che consente di spostare capitali sotto forma di quantità virtuali di oro, sganciandosi, in tale modo, dai problemi valutari del circuito transnazionale⁶⁶.

Non è, però, nota l'incidenza reale di similari metodiche nel contesto generale delle attività di riciclaggio per cui si rende necessario uno studio analitico attento del settore, rifuggendo, al contempo, da talune diffuse semplificazioni, derivate da una proposizione di scenario non sempre fondata su fatti reali e, talvolta, viziata dall'accoglimento di vere e proprie leggende metropolitane.

Esiste anche la possibilità di effettuare il pagamento di beni e servizi attraverso Internet, senza la necessità di utilizzare direttamente la propria carta di credito: tali servizi, dei quali il più noto è *Paypal*⁶⁷, consentono una registrazione dell'utente, che potrà inviare o ricevere denaro in tutto il mondo a destinatari anche anonimi (è richiesta solo l'account *e-mail*), senza dover esporre il proprio numero di carta di credito. Questa intermediazione è nata dalle necessità di sicurezza dell'*@commerce*, in particolare delle aste *online*⁶⁸.

⁶⁴ Per quanto riguarda la realtà italiana, i bonifici internazionali non sono abilitati sui servizi di *Home Banking* di tutti gli istituti di credito, anche se una semplice navigazione su Internet consente di reperire, sul territorio nazionale, strutture finanziarie più avanzate e flessibili, che consentono una totale gestione delle transazioni estere via Web, addirittura su telefono cellulare a tecnologia Wrap, fornendo l'opportuno *software* per la sicurezza.

⁶⁵ Il conto può essere aperto anche per posta, con un saldo minimo di \$3500 e con un onorario di apertura di \$759. Le spese di gestione sono gratuite per depositi superiori a 25.000 franchi svizzeri. Il sito è <http://switzerland.isyours.com>.

⁶⁶ <http://www.e-gold.com>.

⁶⁷ Vedasi il sito <https://www.paypal.com>.

⁶⁸ Una lettura delle investigazioni che il gestore di aste Ebay promuove sulle migliaia di transazioni giornaliere effettuate (vds. <http://pages.ebay.it/help/community/investigates.html>) dimostra che la maggiore preoccupazione è per la sicurezza e l'affidabilità degli

Ciò che va compreso è il fatto che, sostanzialmente, le attività telematiche non cambiano il metodo di base delle dinamiche di riciclaggio ma lo rendono estremamente più agevole e flessibile, innanzitutto azzerando le necessità di spostamento fisico dell'operatore illegale ed il bisogno di possedere una serie di corrispondenti negli Stati esteri da attivare attraverso comunicazioni più facilmente intercettabili.

A questo si somma la caratteristica del cosiddetto tempo reale, che rende estremamente efficienti le procedure di *disintermediazione* delle transazioni effettuate: si deve tener presente il fatto che il possessore di un conto telematico non è assolutamente tenuto ad accedervi dal proprio computer aziendale o casalingo ma può farlo da qualunque postazione collegata alla rete Internet cioè, allo stato attuale, da ovunque desideri. Infatti, taluni tentativi, operati da qualche istituto bancario, di provvedere l'utenza telematica di un *software* di collegamento *ad hoc* da installare sulla macchina e tale da generare una certa fissità nei collegamenti, proprio per la loro complessità sono stati rifiutati dall'utenza e costituiscono un modello superato.

I nuovi sistemi sono configurati per assicurare la totale flessibilità, accettando *in toto* l'architettura del mondo Internet e rifiutando connessioni di tipo proprietario.

Lo stesso collegamento con il *provider* Internet, con la diffusione delle tecnologie *wireless* – che rappresentano la credibile prossima frontiera della Rete⁶⁹ – verrà progressivamente a sganciarsi dai gestori classici della telefonia, che già costituiscono un arcipelago di non facile standardizzazione ai fini della risposta alle esigenze investigative.

Poiché la natura profonda di Internet, derivata dalla sua storia e dalla sua strutturazione, rifugge dai controlli, i requisiti implementativi che facilitano l'utenza e gli aspetti gestionali delle realtà creditizie e del relativo indotto producono anche, in modo inevitabile, la creazione di più vasti spazi di sicurezza per le eventuali attività di riciclaggio.

Infatti, la possibilità di attivare diversi *account*, anche ottenuti con dati informativi di fantasia, sui numerosi *provider* esistenti, incentiva lo spazio operativo dell'eventuale riciclatore cibernetico, rendendo le operazioni di tracciamento molto più complesse.

Per ultimo, nulla vieta di immaginare anche soluzioni tecniche più radicali, quali collegamenti a Internet attraverso un *provider* straniero, attraverso una scheda di telefonia cellulare abilitata per le chiamate internazionali e ottenuta in modo illegale con false attestazioni di identità. Questa

scambi, più che per altri settori di attenzione. Tuttavia, è doveroso segnalare che esiste un protocollo di intesa tra Ebay e le forze dell'ordine dei paesi in cui opera (per l'Italia la Polizia delle Telecomunicazioni), al fine di evitare la commissione di crimini in tale contesto transattivo

⁶⁹ Il 28 maggio 2003 il Ministro delle Comunicazioni on. Maurizio Gasparri ha firmato il decreto tecnico sulle Wireless LAN. Il decreto, che si compone di otto articoli, offre la possibilità agli operatori di fornire servizi di accesso al pubblico su tale architettura, fissandone i criteri.

connessione potrebbe essere facilmente protetta con meccanismi ulteriori, ormai di facile accesso per qualunque utente medio della rete.

Il variegato mondo Internet, a fronte anche della diffusione di cultura antagonista di natura fortemente antistatuale, mette anche a disposizione tecnologie per la totale *anonimizzazione* dell'utente specie attraverso l'uso dei cosiddetti siti *anonimizzer*⁷⁰, che provvedono a farsi carico della transazione Internet⁷¹, depurandola di ogni informazione sull'utente originatore e sulla catena dei *nodi internet* che sta attraversando.

Si sta diffondendo su Internet tutta una serie di siti destinati a supportare, con diverse motivazioni di natura politico/culturale, l'acquisizione di false identità, definite «*Alternate Identity*», per rendersi invisibili alle attività di polizia, ottenendo in modo legale nuove certificazioni di stato civile, passaporti e, per gli USA, *Green Cards* e nuovi *Social Security Numbers*⁷², indispensabili per attività lavorative.

Nella pletera delle risorse della Rete, destinate a chiunque voglia assumere la qualità di *Fakeidman* (uomo dalla falsa identità), esistono anche siti che descrivono minuziosamente la qualità e l'affidabilità dei vari servizi di falsificazione dei documenti e delle attestazioni, consentendo anche ad un utente inesperto di muoversi con meditata ponderazione in un contesto ampiamente, come ovvio, costellato di puri truffatori⁷³.

In sostanza, non appare impossibile mettere in moto meccanismi che conducano all'acquisizione di una falsa identità estera, ottenendo il corrispettivo passaporto⁷⁴: con tale documento sarebbe poi possibile, sempre via Internet, aprire un'azienda in un paese *offshore*, sfruttandone i benefici dati dalla legislazione fiscale e finanziaria. È interessante notare che le compagnie di intermediazione che assicurano tale servizio citano l'obbligo, derivato dalle regole internazionali antiriciclaggio, di *conoscere il proprio cliente*: a tale scopo, viene richiesta una copia del passaporto, assicurando che essa verrà tenuta riservata e resa nota solo dietro un ordine di una Corte di giustizia⁷⁵.

⁷⁰ Molti di questi siti sono posti nelle Repubbliche dell'ex Unione Sovietica. Va distinta la possibilità operativa delle soluzioni a basso costo (vds. il *software A4Proxy*, <http://internet.newfreeware.com/programs/788/>) – che non permettono molte operazioni – da quelle più sofisticate, capaci di offrire una notevole gamma di servizi e di protocolli in totale anonimato. Peraltro, sono ormai disponibili per ogni utente software capaci di cancellare dal proprio computer tutte le tracce delle connessioni effettuate, in modo tale da rendere più complessa l'investigazione tecnica a seguito di sequestro della macchina.

⁷¹ Con un servizio detto di «*proxy*».

⁷² Vedasi, fra i molti, il sito <http://www.undercoverpress.com>, che contiene un vasto assortimento di manualistica dedicata alla costruzione di una falsa identità, supportata da documenti legali ineccepibili.

⁷³ Vedasi il sito <http://www.fakeidman.org>, dove esiste una completa *review* delle risorse disponibili per chi vuole «scivolare» in una identità alternativa.

⁷⁴ È possibile che gli eventi terroristici del 2001 abbiano reso più complesse tali procedure, almeno negli USA.

⁷⁵ Vedasi, a titolo di mero esempio, <http://www.proform.co.uk>, dove si illustrano i servizi offerti di «*Offshore Company Formation Specialists*», alle Bahamas, nel Belize, Isole Vergini, Hong Kong, Mauritius, ecc.. Ognuno di questi paesi viene esaminato, offrendo una sintesi dei vantaggi offerti dal profilo politico, socio/economico, fiscale e giudiziario.

Per quanto riguarda il *cyberlaundering* via Internet, l'implementazione di procedure di controllo preventive, pur non impossibile sotto il profilo tecnologico, si rivela di difficile attuazione per diversi ordini di motivazione: si tratterebbe, infatti, di un'analisi massiva e generalizzata delle comunicazioni sulla rete, al fine di estrapolare quelle che, per natura di protocollo e per destinatario, potrebbero essere configurate come transazioni finanziarie sospette⁷⁶.

In una prospettiva meno ampia ed invasiva, si potrebbe analizzare il traffico delle comunicazioni verso siti sospetti, non allo scopo di decifrare⁷⁷ ed interpretare le singole transazioni ma almeno per trarne degli indicatori statistici generali di rischio, in grado di costituire la base di futuri provvedimenti specifici e mirati su singole fattispecie.

In tal guisa, si potrebbe collazionare in modo selettivo un insieme di comunicazioni a rischio, da sottoporre ad analisi associativa, per estrarne i *pattern* significativi sotto il profilo criminale.

Sulla base del quadro costituzionale e giuridico esistente, tali trattamenti massivi ed indiscriminati dei flussi di comunicazione sul *backbone* Internet non sarebbero percorribili, in assenza di precisi riscontri sull'esistenza specifica di delitti-presupposto in atto: si ritiene, comunque, questo argomento degno di futuri maggiori approfondimenti.

Peraltro, anche dal punto di vista tecnologico, l'infrastruttura dedicata ad una simile analisi dovrebbe essere configurata per supportare in continuità notevolissimi flussi di dati in tempo reale; ciò comporterebbe notevoli investimenti in risorse elaborative ed umane.

Dopo gli attentati dell'11 settembre 2001 esiste in dottrina una chiara, seppur minoritaria, tendenza ad invocare questo controllo preventivo sulla rete Internet: è evidente che una tale problematica si ricollega non solo alle esigenze di sicurezza ma anche ad un progressivo chiarimento istituzionale intorno alla natura giuridica della Rete, natura di carattere sfumato, intorno alla quale si sono sviluppate almeno tre dottrine interpretative.

La prima muove dal postulato secondo il quale Internet sarebbe un mero accorgimento tecnico, una struttura logica, in base alla quale tutti i rapporti telematici non si realizzerebbero *con* la Rete ma *nella* Rete tra soggetti diversi, riconducendola alla nozione di *luogo*.

La nozione naturalistica di territorio non si attaglia ad una realtà virtuale come Internet, dove non è possibile determinare un confine fra le varie reti territoriali che attraversano i singoli Stati; si è allora sviluppato il concetto del c.d. *meta-territorio*, una sorta di territorio virtuale dove i confini fra i vari stati sarebbero non fisici ma logici.

⁷⁶ Esistono talune indagini della Procura della Repubblica presso il Tribunale di Torino, che si sono svolte partendo dall'analisi dei flussi di comunicazione verso siti esteri che detenevano materiale pedo-pornografico. In questo caso, però, l'attività stessa di distribuzione e scaricamento di immagini è prevista come reato dalla norma (art. 600-ter e *quater* c.p.), mentre tale non lo sarebbe, almeno in via presuntiva, un accesso ad un sistema informatico di una banca *offshore*.

⁷⁷ L'uso di sistemi di crittografia rende la decrittazione altamente improbabile.

Tale esplicitazione dottrinale, per quanto fascinosa, mette in luce la fondamentale inadeguatezza a spiegare in modo compiuto la natura giuridica di Internet, rifacendosi ad un concetto (il *meta-territorio*) che non appartiene ad alcun schema classico di interpretazione, anche perché, pur essendo Internet una realtà virtuale, gli effetti dei comportamenti dei soggetti che vi operano si producono nel mondo reale.

La seconda dottrina condivide le posizioni di base della prima ma pone l'accento soprattutto sul concetto di *sovranazionalità* di Internet, più che sulla *trans-nazionalità*, sottolineando il fatto che Internet investe non un singolo Stato ma qualsiasi Stato dotato di una struttura tecnologica adeguata. A tale proposito si sviluppa un nozione di natura giuridica di Internet sulla base dell'inquadramento giuridico dei singoli gestori sparsi nel mondo.

Tale impostazione appare però carente e non risolutiva del problema: infatti, la somma dei regimi giuridici dei singoli gestori dei servizi Internet non può certo considerarsi esaustiva di una realtà che trascende i singoli operatori, peraltro essendo il contesto caratterizzato da pesanti discrasie.

La terza dottrina si fonda prevalentemente sulla "*Dichiarazione di indipendenza del Cyberspazio*"⁷⁸, secondo cui Internet si identifica con uno *spazio logico* (*Cyberspace*), caratterizzato dal fatto che gli utenti possono navigare con totale autonomia rispetto ad ogni autorità statale: in tale modo, non dovrebbero essere riconosciuti i concetti giuridici tradizionali, quasi dotando la Rete di una dichiarata, anarchica immunità ad ogni controllo.

Più che una soluzione specifica, queste dottrine mettono in luce la necessità di definire Internet in relazione alla individuazione della legge applicabile per la disciplina della rete e delle relazioni virtuali: problemi di non facile soluzione, perché le norme per l'individuazione della legge applicabile e del giudice competente sono sempre state elaborate con precisi riferimenti ad uno spazio fisico e territoriale.

Una soluzione al problema dovrà essere raggiunta per passi successivi e non potrà che realizzarsi in ambito internazionale, attraverso stipulazione di trattati e convenzioni ad ampia partecipazione di Stati, sia in tema di uniformità di norme sostanziali che di conflitto, nell'ottica pratica di una regolamentazione del fenomeno.

2.6 Il riciclaggio nel sistema penale e processuale italiano

La vigente legislazione, sviluppata negli anni, mette a disposizione una vasta gamma di ipotesi sanzionatorie e di possibilità strumentali preventive, investigative e processuali per il contrasto ai fenomeni di riciclaggio, avendo bene presente l'importanza primaria del controllo e della tutela del circuito bancario e finanziario, così come la necessità di individuare speciali possibilità di intervento, per l'acquisizione di più estese

⁷⁸ Promulgata da John Perry Barlow a Davos, in Svizzera, l'8 febbraio 1996.

fonti di prova sui circuiti associativi criminosi e non solo sulle singole manifestazioni dello specifico reato.

La gestione di somme provenienti da illeciti concretizza, secondo i casi, diverse ipotesi di reato, punite dagli articoli 648 (*ricettazione*), 648-bis (*riciclaggio*), 648-ter (*impiego di denaro, beni o utilità di provenienza illecita*) c.p..

Nel delitto di riciclaggio si punisce «chi, fuori dai casi di concorso, sostituisce o trasferisce denaro, beni o altra utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa», mentre il 648-ter vieta «l'impiego, fuori dai casi di concorso, in attività economiche o finanziarie di denaro, beni od altra utilità provenienti da delitto»: il termine *sostituisce*, che descrive l'attività sostanziale del riciclaggio, comprende anche il deposito bancario, mentre il *trasferimento* comprende sia trasferimenti senza sostituzione, atti solo a far scemare la «*pista di carta*», sia anche il mero spostamento dei beni, come nelle attività dei corrieri.

Il comportamento deve essere idoneo ad ostacolare l'identificazione dell'origine delittuosa dei beni e, quindi, può comprendere anche il comportamento dell'operatore bancario, che, avendo la sostanziale certezza della provenienza criminosa dei beni, ugualmente perfeziona la transazione, al fine di ostacolare le indagini dirette alla ricostruzione della filiera del flusso finanziario: come si vede, questa ipotesi deve essere abbondantemente provata, ricadendo, invece, le condotte omissive sotto diversa normativa, della quale si dirà nel prosieguo.

Le condotte di cui ai precitati artt. 648-bis e 648-ter non sono riconducibili alle attività di riciclaggio *primarie* poste in essere dagli attori del sodalizio criminale, che ha prodotto l'illecita ricchezza: esse sono, invece, condotte complementari, *secondarie* al delitto presupposto e realizzate da soggetti diversi ed estranei.

Le indagini sul riciclaggio dovranno dunque essere collegate alle indagini sul circuito criminoso che ha prodotto la ricchezza illecita e alle indagini sui meccanismi di *riciclaggio primario* posto in essere nell'ambito di quei sodalizi: una volta ben radicata questa ipotesi di base, le indagini sul riciclaggio di cui ai predetti articoli potrà assumere anche una valenza autonoma, sia nei confronti di singoli, che di strutture associative (art. 416 c.p.) finalizzate alla commissione di tale reato.

Da ciò si deduce che un appartenente ad associazione mafiosa *ex art. 416-bis*, che sia dedito a riciclare i capitali illeciti del sodalizio, non potrà ricadere nella sfera di applicabilità del 648-bis: le sue condotte di riciclaggio primarie fanno infatti parte delle condotte di partecipazione al sodalizio mafioso.

La confidenzialità delle informazioni bancarie è un obbligo tutelato dalla norma, che è stato anche recentemente riaffermato dal Garante della *privacy*, in un suo provvedimento del 23 maggio 2001, che appare opportuno citare, quale ben meditata sintesi del contesto giuridico di riferimento:

«Tale obbligo, comunemente configurato come connaturato al rapporto banca-cliente in applicazione dei principi di correttezza e buona fede nell'esecuzione del contratto (artt. 1175, 1375 e 1337 del codice civile), è anche espressamente richiamato o presupposto da diverse disposizioni normative in materia fiscale e tributaria o in materia di riciclaggio, in relazione ai poteri di accertamento che permettono a determinati soggetti pubblici di acquisire notizie ed informazioni presso istituti di credito (v., ad es., l'art. 10, comma 2, n. 12) della l. 9 ottobre 1971, n. 825; l'art. 4 l. 9 agosto 1993, n. 328 di ratifica della convenzione di Strasburgo sul riciclaggio dell'8 novembre 1990; le norme sull'anagrafe dei rapporti di conto e di deposito, di cui all'art. 20, comma 4, l. n. 413/1991 e al D.M. 4 agosto 2000, n. 269 del Ministro del tesoro, del bilancio e della programmazione economica; Corte cost. 3-6 luglio 2000, n. 260 e Cass. Civ. Sez. I, 7 agosto 1990, n. 7953, in materia di ordine di esibizione rivolto dal giudice civile ad un istituto di credito; v. anche la deliberazione Consob n. 11522/1998 di attuazione del D.lg. n. 58/1998, che impone al personale delle banche e degli altri intermediari precisi obblighi di riservatezza sulle informazioni di carattere confidenziale acquisite dagli investitori o di cui si disponga in ragione della propria funzioni.

I doveri di confidenzialità connessi al c.d. segreto bancario trovano anche riscontro negli usi e nelle consuetudini bancarie, nonché negli impegni che gli istituti di credito assumono nei confronti della clientela allorché dichiarano di rispettare le regole di comportamento indicate dalla relativa associazione di categoria, anche per ciò che attiene alla riservatezza nella raccolta e nel trattamento delle informazioni sui clienti (v. il Codice di comportamento del settore bancario e finanziario predisposto dall'Associazione bancaria italiana, parte I e parte IV, punto 2 [...] nonché il codice di autodisciplina deliberato dall'A.B.I. in tema di intermediazione finanziaria, punto 1... v. inoltre l'art. 11 del C.C.N.L. del 22 giugno 1995, relativo al personale direttivo delle banche che stabilisce il divieto per il funzionario di comunicare notizie riservate di ufficio). [...] Da quanto sopra esposto, emerge che, fuori dei casi di operazioni di comunicazione di dati connesse alle prestazioni richieste o ai servizi erogati (e dei casi di adempimento di obblighi normativi in base ai quali gli istituti di credito devono fornire determinate informazioni a soggetti pubblici), gli istituti stessi ed il relativo personale devono mantenere il riserbo sulle informazioni relative ai propri clienti e non divulgarle a terzi».

In tema di indagini bancarie, particolare rilievo assume la norma del secondo comma dell'art. 248 c.p.p., che consente all'Autorità Giudiziaria il potere di delegare agli ufficiali di P.G. la ricerca presso le banche per «esaminare atti, documenti e corrispondenza».

È stato evidenziato un problema interpretativo, offerto dall'art. 248, comma 2, sulla delegabilità o meno delle perquisizioni da parte dell'Autorità Giudiziaria, in conseguenza del rifiuto posto in essere dalla banca al rintraccio di «cose da sottoporre a sequestro» o all'accertamento di «circostanze utili ai fini delle indagini», in quanto il citato comma - con no-

tevoli implicazioni pratiche – statuisce che «in caso di rifiuto l’Autorità Giudiziaria procede a perquisizione».

Se si accogliesse la tesi della non delegabilità in caso di rifiuto, si concederebbe alle banche il singolare potere di eliminare l’effettiva possibilità di svolgere indagini in modo aderente alla situazione e si consentirebbe l’uso di tale espediente da parte degli istituti di credito condizionati dalle organizzazioni criminali o che intendono evitare l’accertamento di situazioni illecite⁷⁹.

L’art. 255 c.p.p. regola il sequestro presso le banche, per quanto attiene documenti, titoli (di qualunque specie), valori (di ogni tipo: denaro, moneta, preziosi), somme depositate in conto corrente (o a risparmio) e ogni altra cosa, anche se contenuta in cassette di sicurezza.

Inoltre, nell’art. 255 c.p.p., non esiste traccia di limitazioni di delega da parte dell’A.G. agli ufficiali di P.G., simili a quelle ventilabili nell’art. 248, il che offre minori difficoltà interpretative.

L’aspetto più interessante dell’art. 255 c.p.p. è che sussistono i presupposti ricordati; è possibile operare un sequestro di cose, valori o documenti «quantunque non appartengono all’imputato o non siano iscritti al suo nome».

Inoltre, ai sensi dell’art. 321, comma 2, c.p.p., nel corso di indagini preliminari sui delitti previsti dal 648-*bis* e *ter*, può operarsi il *sequestro preventivo*.

A seguito di condanna, è particolarmente importante l’art. 12-*sexies* della legge 356 del 1992, che consente di confiscare denaro, beni od altra utilità, dei quali il condannato «non può giustificare la provenienza e di cui, anche per interposta persona fisica o giuridica, risulta essere titolare o avere la disponibilità a qualsiasi titolo in valore sproporzionato al proprio reddito, dichiarato ai fini dell’imposte sul reddito o alla propria attività economica». In tale modo, si rendono aggredibili anche quei patrimoni criminali, la cui origine delittuosa sarebbe difficile dimostrare, in virtù del fatto che si sposta, giustamente, sul condannato l’onere di provare che la ricchezza sproporzionata rispetto al reddito sia riferibile a provenienza legittima.

Inoltre, con riferimento ai delitti previsti dagli artt. 648-*bis* e 648-*ter* c.p., è stata introdotta, con l’art. 10 della legge n. 172 del 1992, una norma derogatoria di principi generali in materia di misure cautelari⁸⁰:

⁷⁹ Vedi Antonio Laudati «*Terrorismo internazionale, criminalità organizzata e money transfer*» sulla rivista del SISDE *Per aspera ad veritatem*, n. 24 del 2002.

⁸⁰ «Quando è necessario per acquisire rilevanti elementi probatori ovvero per la individuazione o cattura dei responsabili dei delitti di cui agli artt. 629, 648-*bis*, 648-*ter* c.p., il Pubblico Ministero può, con decreto motivato, ritardare l’esecuzione dei provvedimenti che applicano una misura cautelare, dell’arresto, del fermo dell’indiziato di delitto o del sequestro. Nei casi di urgenza il ritardo dell’esecuzione dei predetti provvedimenti può essere disposto anche oralmente, ma il relativo decreto deve essere emesso entro le successive 48 ore. Per gli stessi motivi di cui al comma 1 gli ufficiali di polizia giudiziaria possono omettere o ritardare gli atti di propria competenza, dandone immediato avviso, anche oralmente, al pubblico ministero competente per le indagini, e provvedono a trasmettere allo stesso motivato rapporto entro le successive 48 ore»