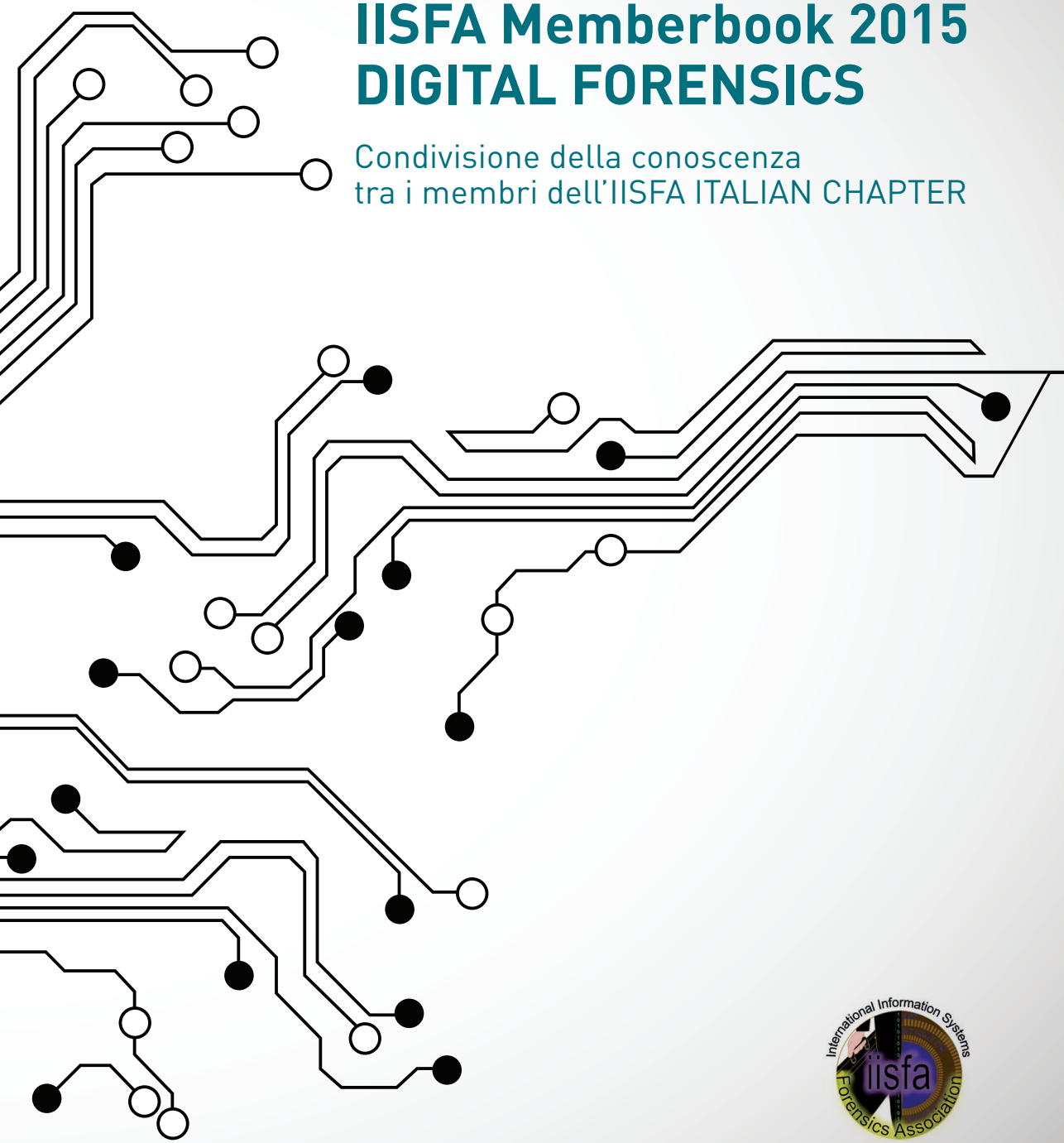
a cura di
Gerardo Costabile - Antonino Attanasio - Mario Ianulardo

IISFA Memberbook 2015
DIGITAL FORENSICS

Condivisione della conoscenza
tra i membri dell'IISFA ITALIAN CHAPTER



PREFAZIONE

Cari Soci, Cari Amici dell'IISFA,
grazie allo sforzo congiunto degli Autori e dei Curatori, che di buon grado hanno collaborato allo scopo di consegnare per tempo i loro lavori, questa edizione annuale del Memberbook 2015 è giunta entro la fine dell'anno 2015.
Anche quest'anno, è stato denso di avvenimenti di rilievo per la nostra Associazione:

- abbiamo effettuato una Survey per reperire informazioni e spunti per il miglioramento dell'associazione e dei suoi meccanismi interni ed esterni;
- ci sono stati cambiamenti nella governance dell'associazione (4 membri del Board hanno lasciato spazio ad altri soci che hanno garantito un ricambio anche generazionale, durante elezioni svoltesi il 15 maggio 2015);
- è stato dato patrocinio al "DFA (Digital Forensics Alumni) Open Day 2015" (Milano 2 luglio), al seminario "I Reati di Oggi: Informatici e Telematici" (Velletri RM 22 Giugno) con intervento "Pedopornografia e adescamento di minorenni" a cura di Mario Ianulardo, all'evento "ICT Certification Day" (Roma 15 settembre) con intervento sulla CIFI da parte di Francesco Scarpa, al seminario "Le investigazioni: aspetti giuridici e informatici" (Amelia TR 1 ottobre) con intervento "Pedopornografia e adescamento di minorenni" a cura di Mario Ianulardo, al "Forum ICT Security 2015" (Roma 15 e 16 ottobre) con la partecipazione di Gerardo Costabile alla tavola rotonda "La convergenza della sicurezza fisica e logica come elemento chiave di una strategia per l'ICT";
- è stato organizzato il seminario di aggiornamento professionale "Le indagini di polizia giudiziaria nell'era delle innovazioni tecnologiche – esperienze operative a confronto" (Ancona 4 dicembre);
- abbiamo collaborato con l'Università degli Studi del Molise nell'ambito della IV edizione del Master universitario di I livello in "Sicurezza Informatica e Digital Forensics";
- abbiamo partecipato al Security Summit di Roma organizzando un seminario IISFA nella giornata dell'11 giugno, in cui ci sono stati gli interventi di Giuseppe Dezzani "Dall' acquisizione del device all'analisi dei dati e dei tabulati di traffico" e di Stefano Aterno "Il valore probatorio dei documenti e della posta elettronica nelle indagini informatiche: aspetti giuridici e giurisprudenziali di tali acquisizioni forensi anche alla luce delle nuove norme introdotte con la legge Antiterrorismo (art. 234 bis c.p.p)" con Gerardo Costabile come moderatore;
- formazione con rappresentanti dell'associazione presso alcuni

Master universitari di particolare pregio (si cita, in particolare, il Master di Scienze Forensi, Intelligence e Sicurezza dell'Università La Sapienza, con il coordinamento del Prof. Avv. Natale Fusaro).

Anche nel 2015 si è tenuto il consueto appuntamento annuale IISFA Forum & CyberCop Challenge, questa volta a Roma presso la Casa dell'Aviatore nei giorni 15 e 16 maggio.

L'attività seminariale riservata per i soci è stata molto intensa:

- Milano 27 febbraio: Open Source Intelligence & Web investigation-Social Network Analysis;
- Milano 20 marzo: Malware Analysis – Le intercettazioni 2.0;
- Milano 24 aprile: Computer e Mobile Forensics;
- Milano 22 maggio: Bitcoin Forensics e Deep Web;
- Milano 10 luglio e 11 settembre: 2 Laboratori di Computer Forensics e Mobile forensics;
- Roma 18 settembre: Analisi dei dati e dei tabulati di traffico, chip off e camera bianca;
- Roma 23 ottobre: Malware Analysis - Le intercettazioni 2.0;
- Roma 20 novembre: Open Source Intelligence & Web investigation - Social Network Analysis;
- Roma 11 dicembre: Acquisizione delle evidenze informatiche – Deep Web;
- Roma dicembre: 2 Laboratori di Computer Forensics e Mobile forensics.

Per l'anno 2016 gli obiettivi deliberati dal Board nel mese di giugno scorso sono i seguenti:

- rafforzare ulteriormente le attività formative e seminariali, anche tramite e-learning;
- revisionare i contenuti del sito IISFA;
- rinnovare e rafforzare la certificazione CIFI.

Ricordo a tutti, prima di tutto a me stesso, che l'Associazione è la somma di noi tutti, come i semi di un melograno.

Tanti semi, unico frutto.

Ringrazio tutti i soci che hanno rinnovato la fiducia nella nostra associazione ed in particolare quelli che, dentro e fuori al board, supportano le attività gestionali day by day.

Ad maiora.

Il Presidente
Gerardo Costabile

Capitolo I

LE TRUFFE SU PIATTAFORMA DI *E–COMMERCE*: L'ESPERIENZA DELLA PROCURA DI MILANO

Francesco Cajani[1], Fabio Cavallo[2]

Sommario:

1. IL FENOMENO ILLECITO: DEFINIZIONI GENERALI

Le truffe su piattaforma di *e–commerce* sono quelle poste in essere attraverso l'utilizzo di siti web specializzati nella vendita online di beni e/o servizi (ad esempio *www.ebay.it*, *www.subito.it*, *www.autoscout24.it*, *www.kijiji.it* e tanti altri) ovvero anche tramite siti appositamente creati per finalità illecite. In sostanza il truffatore finge di mettere in vendita un bene al solo scopo di ottenere dal potenziale acquirente il pagamento di una somma di denaro attraverso bonifici a favore di

1 Paragrafi 3, 4 e 6. "*Dedicato a Manlio Minale, recentemente scomparso, per avermi generosamente supportato in questa faticosa ma fondamentale esperienza professionale*".
2 Paragrafi 1, 2 e 5.

conti correnti ovvero tramite ricariche di carte di credito prepagate o anche attraverso l'utilizzo diretto delle carte di credito tradizionali, o ancora tramite vaglia postali. Una volta ricevuto il denaro, il venditore fa perdere le proprie tracce senza chiaramente inviare all'acquirente il bene posto in vendita, oppure inviando un bene totalmente diverso o comunque non funzionante.

Allo stesso modo, sempre più frequenti sono le truffe relative all'affitto di appartamenti per vacanze: anche in tale ipotesi il truffatore finge di avere simili disponibilità di beni, che pone in visione in Rete tramite appositi annunci. Si tratta peraltro, come vedremo in seguito, di appartamenti spesso effettivamente esistenti, in relazione ai quali il truffatore abbina però – quanto ai dati relativi alla proprietà – il nome di persone ignare, vittime di furto di identità.

Meno numerosi, ma ugualmente degni di nota, sono i casi nei quali il truffatore, generalmente uno straniero, assume la parte dell'acquirente. In pratica egli acquista un bene che paga inviando al venditore un assegno (quasi sempre emesso da banche estere) apparentemente regolare ma in realtà falsificato. In questi casi viene sfruttata la lentezza dei meccanismi bancari nell'accertare la falsità del titolo di credito: infatti il venditore versa sul proprio conto corrente l'assegno ricevuto (che viene di regola subito accettato dalla propria banca) ma quando l'istituto di credito, dopo qualche giorno, si accorge che l'assegno è falsificato e avverte il venditore, è ormai troppo tardi perché il bene è già stato inviato al truffatore.

Quale variante di tale ultimo *modus operandi*, ci sono casi nei quali l'assegno utilizzato, oltre che falso, è anche di un importo superiore al prezzo pattuito. Alla luce di tale presupposto il truffatore, accampando giustificazioni apparentemente verosimili quali l'essere incorso in un errore, chiede al venditore che gli venga restituita la somma eccedente attraverso il meccanismo del trasferimento di denaro via Western Union. In questi casi quindi il profitto conseguito dal truffatore è doppio: non solo riceve un bene che di fatto non ha pagato, ma anche denaro contante immediatamente utilizzabile.

In genere la somma di denaro che viene ricavata per ogni singolo episodio truffaldino non è elevatissima (al massimo poche centina di euro: vedi *infra* par. 4): in effetti l'obiettivo dei truffatori è raggiungere un elevato profitto (in alcuni casi anche elevatissimo) portando a termine un gran numero di truffe, puntando quindi soprattutto sulla quantità; ciò consente loro anche di sperare che le proprie vittime desistano dal proporre querela, scoraggiate dal fatto che un eventuale procedimento penale a carico del responsabile, comporterebbe per loro fastidi e costi sicuramente superiori al denaro perduto, anche in considerazione del fatto che, alla fine, è spesso molto difficile riuscire ad ottenere un risarcimento, anche qualora il responsabile fosse condannato[3].

3 Si rinvia, sul punto, al working paper "*Vittimɑ ineffabile*" reperibile all'indirizzo *www.procura.milano.giustizia.it/vittima–ineffabile.html.*

Come verrà approfondito nel prosieguo (cfr. par. 4), al pari di tutti gli altri tipi di truffe anche quelle commesse su piattaforme di *e–commerce* si perfezionano nel momento in cui si verifica il conseguimento del profitto da parte del reo, corrispondente alla *deminutio patrimonii* della vittima: in sostanza quando quest'ultima effettua il pagamento del bene a favore del sedicente venditore. Tuttavia occorre precisare che le modalità attraverso le quali avviene tale pagamento costituiscono un elemento fondamentale per definire questo tipo di truffe, in quanto il passaggio di denaro deve avvenire – per definizione – senza un contatto fisico tra le parti. Pertanto, se il truffatore e la sua vittima, dopo i primi contatti tenuti attraverso Internet, convengono di incontrarsi per perfezionare la compravendita con la consegna del bene da parte del venditore e il pagamento in contanti da parte dell'acquirente, a rigore non siamo più di fronte ad una truffa su piattaforma di *e–commerce*, proprio perché essa non si è perfezionata in Rete, ma appunto durante l'incontro. Ciò avviene nei casi in cui il truffatore venditore consegna un bene apparentemente regolare e funzionante (di solito un telefono cellulare) che invece dopo qualche giorno smette di funzionare (ad esempio perché viene bloccato essendo stato acquistato a rate che non sono mai state pagate); oppure quando il truffatore acquirente del bene consegna nelle mani del venditore un assegno apparentemente valido, ma in realtà falsificato o rubato.
In definitiva è possibile affermare che se è indispensabile, per definire le truffe commesse su piattaforma di *e–commerce*, che i contatti tra le parti avvengano in Rete, ciò non è tuttavia sufficiente, essendo altresì necessario anche che la truffa si perfezioni senza alcun contatto fisico diretto tra vittima e truffatore.

2. CLASSIFICAZIONE DELLE DIVERSE TIPOLOGIE DI TRUFFE SU PIATTAFORMA DI E–COMMERCE

Quelle appena descritte sono evidentemente le ipotesi più semplici di questo tipo di reati, atteso che la consolidata esperienza della Procura di Milano nel contrasto a questi fenomeni ha permesso di verificare che nel corso degli anni il *modus operandi* dei truffatori ha subito una vera e propria evoluzione, chiaramente finalizzata a rendere sempre più difficile l'individuazione dei responsabili da parte degli organi inquirenti, sfruttando da una parte l'inesperienza e l'ingenuità degli utenti della rete, dall'altra la vulnerabilità del mezzo informatico. In questo senso la comparsa di nuovi metodi di pagamento (come i conti correnti e le carte di credito attivabili esclusivamente online, le carte di credito non nominative al portatore, o anche metodi di trasferimento di denaro come Western Union o Money Gram), più aleatori rispetto a quelli tradizionali, ha oggettivamente agevolato la realizzazione di questo tipo di truffe.
È possibile pertanto individuare alcune varianti delle truffe su piattaforma di *e–commerce* che di seguito verranno analizzate.

2.1 Truffe commesse da un singolo individuo

Si tratta delle ipotesi più elementari di questo tipo di truffe, portate a termine da un singolo individuo che, approfittando del mezzo informatico e sentendosi protetto dall'anonimato che spesso contraddistingue chi ne fa uso, ed inoltre facendo affidamento sulla lunghezza delle indagini, porta a termine il proprio disegno criminoso, convinto che difficilmente verrà scoperto dagli inquirenti. Il truffatore può essere:

a. un giovane, generalmente abile nell'utilizzo del computer, che porta a termine le truffe per guadagnare soldi facili; in questi casi il numero di truffe portate a termine da ogni singolo truffatore può essere anche molto basso; anzi capita che il giovane, dopo aver portato a termine la prima truffa, si fermi nel suo disegno criminoso per ridurre il rischio di essere individuato, accontentandosi dei soldi ricavati nella prima occasione e soddisfatto di aver comunque dimostrato a se stesso e ai suoi amici, di essere capace di fare col computer ciò che vuole;

b. un adulto, di solito in difficoltà economiche, che utilizza le truffe per sovvenzionare le proprie dipendenze (droga, alcool, gioco d'azzardo); in questi casi invece le truffe portate a termine sono spesso molto numerose, proprio perché il responsabile ha un continuo bisogno di soldi che riesce a soddisfare soltanto perpetuando il suo disegno criminoso. In sostanza siamo di fronte ad un "truffatore seriale";

c. un truffatore "di professione", dedito al compimento di ogni tipo di truffe, che trova in quelle su piattaforma di *e–commerce* una ulteriore possibilità per realizzare profitti. Anche in questo caso siamo di fronte ad un truffatore seriale, essendo notevolmente alto il numero delle truffe commesse da ogni singolo individuo, in linea con la personalità criminale di questo tipo di truffatori, che tendono a credersi invulnerabili e a fare delle truffe la loro ragione di vita.

2.2 Truffe commesse da organizzazioni criminali

Negli ultimi tempi si sono moltiplicati i casi di truffe perpetrate da vere e proprie organizzazioni criminali composte da più persone, ad ognuna delle quali è affidato un compito preciso nell'ambito del disegno criminoso.
Sono organizzazioni che portano a termine un gran numero di truffe che consentono di ricavare ingenti somme di denaro (a volte anche dell'ordine di milioni di euro). Si tratta spesso di stranieri domiciliati in Italia che poi trasmettono all'estero i soldi guadagnati, ma ci sono stati anche casi rilevanti di organizzazioni formate anche da italiani, i cui legami con la criminalità organizzata tradizionale sono meritevoli di attenta analisi da parte degli organi inquirenti, dal momento che il settore delle truffe su piattaforma di *e–commerce* può costituire un metodo efficace, e per certi versi innovativo, per le attività di riciclaggio e di *"pulizia"* del denaro sporco.

a. Al vertice di tali associazioni criminali ci sono ***gli organizzatori***, in sostanza i personaggi che si occupano di predisporre la struttura criminale, coordinare tutte le attività necessarie per portare a termine le truffe e gestire i guadagni. Sono in genere coloro che rimangono sempre nell'ombra, protetti dalla rete organizzativa che essi stessi predispongono. In sostanza sono coloro che hanno la piena disponibilità dei conti correnti e/o delle carte di credito (di cui posseggono tutti i codici di accesso), sui quali giunge in definitiva il denaro ricavato dalle truffe. Non sempre tali conti e tali carte corrispondono a quelli a favore dei quali le vittime delle truffe eseguono i rispettivi pagamenti, essendo possibile infatti che venga predisposto un ulteriore passaggio di soldi verso altri rapporti bancari e postali, ciò al fine di rendere l'organizzazione sempre più ramificata e rendere così più complicata l'individuazione della destinazione finale del denaro.
b. Nella posizione intermedia c'è quella che potremmo definire, in termini non giuridici, ***"la manovalanza"***, di cui fanno parte tutti coloro che concretamente portano a termine le truffe, portando avanti le contrattazioni e mantenendo i contatti con i potenziali acquirenti, attraverso il mezzo informatico e varie utenze telefoniche appositamente attivate. Alcune volte sono gli stessi organizzatori ad espletare tali funzioni, ma più spesso vengono arruolate a tal fine altre persone le quali vengono ricompensate con una percentuale sui guadagni. Anche in questo caso siamo di fronte al tentativo di rendere sempre più complessa la struttura e rendere così più difficile il compito degli inquirenti, senza contare il fatto che, in questo modo, gli organizzatori si sentono più protetti qualora l'attività investigativa riuscisse a risalire al primo grado della struttura criminale.
   Spesso vengono arruolate anche persone molto abili nell'utilizzo illecito del mezzo informatico, le quali si occupano esclusivamente di garantire all'organizzazione collegamenti telematici "sicuri", attraverso accessi abusivi ai sistemi informatici di ignare persone, i cui computer e i cui collegamenti telefonici, privi di un sufficiente sistema di protezione, vengono utilizzati, a loro completa insaputa, per la registrazione sulle piattaforme di *e–commerce*, nonché per la creazione e la successiva utilizzazione di account di posta elettronica indispensabili per i contatti con le vittime.
c. Infine, alla base della organizzazione, ci sono tutti coloro che risultano ***intestatari delle utenze*** telefoniche (mobili e fisse) utilizzate per mantenere i contatti con i potenziali acquirenti, ***nonché dei rapporti bancari e/o postali*** (conti correnti aperti allo sportello, conti correnti attivati online, carte di credito prepagate ricaricabili emesse dalle banche, postepay, ecc.) a favore dei quali le vittime sono indotte ad effettuare i pagamenti. Anche se spesso le persone che risultano intestatarie delle utenze telefoniche e dei rapporti bancari e/o postali sono completamente ignare di tutto, essendo esse stesse vittime di furto di identità e sostituzione di persona, molte volte invece capita che i personaggi che fanno parte della manovalanza vadano alla ricerca di persone (in genere individui ai margini della società, indi-

genti, senza fissa dimora, stranieri clandestini, ma anche persone facilmente influenzabili perché affette da ritardi mentali) le quali, in cambio di una piccola ricompensa (che in genere non supera i 100 euro), vengono convinte ad attivare a loro nome le utenze telefoniche e, soprattutto, le carte di credito e i conti correnti che verranno poi utilizzati per compiere le truffe. È chiaro che in questi casi, tutti i codici di accesso e le stesse carte di credito vengono immediatamente consegnati all'organizzazione dagli intestatari i quali pertanto non ne hanno mai la reale disponibilità.

2.3 Truffe commesse tramite sostituzione di persona

L'esame delle truffe poste in essere dalle organizzazioni criminali ha introdotto un ulteriore elemento che, con il passare degli anni, è diventato sempre più centrale in questo tipo di attività criminosa: il furto di identità e quindi la realizzazione delle truffe su piattaforma di *e–commerce* mediante sostituzione di persona. Si tratta in sostanza dell'espediente principale utilizzato dai truffatori per rendere più lunghe e complicate le indagini su questo tipo di fatti criminosi in quanto consente di agire con più sicurezza almeno fino a quando esso non viene accertato dalle indagini, che in ogni caso sono rese più lunghe e più complicate. Posto che la sostituzione di persona può essere attuata evidentemente sia dal truffatore singolo, sia dalle organizzazioni criminali, non si può non rilevare come siano state proprio queste ultime a perfezionarne le modalità di attuazione e ad utilizzarla in maniera sempre più rilevante per compiere le truffe.
L'attività preliminare per compiere il furto di identità è carpire tutti i dati sensibili di un'altra persona che poi saranno utilizzati per portare a termine le truffe a suo nome.
I metodi utilizzati a tal fine dai truffatori sono molteplici. A titolo di esempio, quello che nel corso degli anni è stato più comunemente utilizzato consiste nel fingersi interessati all'acquisto di un bene regolarmente posto in vendita sui siti specializzati. Durante i contatti attraverso i quali avviene la contrattazione, il finto acquirente chiede al venditore che, a titolo di garanzia e a dimostrazione della sua serietà, questi gli trasmetta via mail la copia del proprio documento di identità, oltre a comunicargli tutti i dati relativi alle coordinate bancarie (o postali) indispensabili per effettuare il pagamento. Una volta ottenuti dall'ignaro venditore tutti i dati necessari, il finto acquirente interrompe ogni contatto avendo ormai a disposizione tutte le informazioni di cui aveva bisogno.
Un altro espediente adoperato per indurre la vittima a comunicare ogni suo dato sensibile e a trasmettere la copia dei propri documenti, consiste nella vendita online di telefoni cellulari completi di schede telefoniche. In questi casi il truffatore ha interesse a concludere regolarmente la vendita (proprio perché l'acquirente non deve sospettare di nulla), ma chiede alla sua vittima la copia dei documenti di identità fingendo che siano indispensabili per l'attivazione della scheda abbinata al telefono.

Come già accentato, negli ultimi tempi è stato invece verificato a tal fine l'utilizzo sempre più frequente del metodo che consiste nell'affitto online di appartamenti per vacanze in realtà inesistenti o comunque non disponibili. Una volta conclusa la contrattazione, il finto locatore chiede alla sua controparte la copia dei documenti necessari per compilare il contratto di locazione, oltre che una caparra per bloccare l'appartamento. In questo caso quindi, l'aspirante locatario è doppiamente vittima: della truffa, avendo pagato la caparra per l'affitto di un appartamento inesistente; del furto di identità, poiché i suoi dati sensibili saranno utilizzati in seguito per compiere truffe analoghe a suo nome.

Altrettanto molteplici sono le modalità con le quali, una volta carpiti tutti i dati necessari, questi vengono poi utilizzati per portare a termine le truffe a nome delle vittime. Esse possono così essere riassunte:

a. Utenza eBay (o di altra piattaforma di *e–commerce*) intestata ad altra persona.
Il truffatore crea un *account* su eBay (o su un'altra piattaforma di *e–commerce* simile), fornendo generalità, indirizzi e recapiti telefonici della persona a cui ha carpito i dati sensibili di regola tramite *phishing*[4]. Proprio attraverso tale *account* egli pubblica le finte offerte di vendita online per portare a termine le sue truffe.
La persona a nome della quale è stato creato l'*account* si accorge di essere vittima di furto di identità e sostituzione di persona soltanto quando comincia a ricevere le telefonate di sollecito e di protesta da parte delle vittime delle truffe che non vedono arrivare il bene da loro acquistato, oppure quando la società eBay invia al suo indirizzo la richiesta di pagamento per le inserzioni effettuate; in ogni caso dopo un ragguardevole periodo di tempo, durante il quale il truffatore ha la possibilità di agire indisturbato per compiere numerose altre truffe a nome di un'altra persona.
In questi casi il responsabile porta a termine tali truffe inducendo le sue vittime a effettuare i rispettivi pagamenti attraverso l'invio di denaro mediante Western Union (per riscuotere il denaro è sufficiente conoscere il numero della operazione che viene comunicato dalla stessa vittima); oppure attraverso vaglia postali (che il truffatore riscuoterà mostrando documenti falsi); ovvero attraverso il versamento di denaro su conto corrente o carta di credito ricaricabile, attivati sempre a nome della stessa persona vittima del furto di identità che si ritrova quindi, a sua completa insaputa, a risultare intestataria sia di un *account* eBay, sia del rapporto bancario attivato online.

4 Trattasi, come noto, di un metodo illecito molto utilizzato che sfrutta una tecnica di ingegneria sociale: il malintenzionato effettua un invio massivo di messaggi di posta elettronica che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio (quale il proprio sistema di home banking). Per la maggior parte è una truffa perpetrata usando la posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS etc.

b. Conto corrente e/o carta di credito prepagata attivati online e intestati ad altra persona.
Il truffatore attiva un conto corrente online (o anche una carta di credito) utilizzando i dati e la copia dei documenti personali illecitamente carpiti ad altre persone. Come è noto per completare l'attivazione online di un conto o di una carta di credito prepagata è sufficiente inviare alla banca la copia dei documenti di identità e fornire le coordinate di un altro conto corrente aperto in precedenza presso un altro istituto bancario (cosiddetto "*conto corrente di appoggio*" che serve alla banca online come garanzia[5]). Le truffe su piattaforma di *e–commerce* pertanto vengono portate a termine proprio inducendo le vittime a effettuare il pagamento con un bonifico sul conto (o una ricarica della carta di credito) di cui il truffatore, pur non essendone l'intestatario, ha però il totale controllo essendo in possesso di tutti i codici di accesso. È evidente che in tali casi l'*account* di eBay (o di altra piattaforma di vendita online) utilizzato per pubblicare l'offerta di vendita, può essere creato anche attraverso nomi e recapiti di fantasia, che di solito non vengono controllati dalle società che gestiscono il sito, le quali infatti non sono obbligate a farlo.

c. Conto corrente e/o carta di credito prepagata attivati con documenti di identità falsi.
Il *modus operandi* del truffatore è sostanzialmente quello descritto nel punto precedente; in questo caso però il conto corrente o la carta di credito vengono attivati con documenti falsificati. Questo metodo viene posto in essere quando i conti o le carte di credito non vengono attivati online, ma direttamente allo sportello bancario o postale, poiché per farlo è necessario mostrare all'operatore il documento cartaceo (non essendo sufficiente la copia). Il truffatore quindi utilizza un documento originale intestato ad altra persona (di cui è venuto in possesso per averlo rubato in precedenza, o perché lo ha casualmente rinvenuto dopo che l'intestatario lo ha smarrito) al quale ha tolto la fotografia originale, sostituendola con un'altra con la propria effige. È evidente che la falsificazione può interessare anche altri dati presenti sul documento (numero, data di rilascio, generalità dell'intestatario, ecc.).
A volte (soprattutto nei casi di truffe commesse dal singolo individuo) il responsabile utilizza il proprio documento di identità che egli stesso ha in precedenza falsificato modificando i dati delle proprie generalità (nome e cognome e/o data di nascita e/o luogo di nascita e/o luogo di residenza). Di solito ciò avviene dopo che il truffatore ha presentato una finta denuncia di furto o di smarrimento del proprio documento. In questo caso non siamo di fronte ad un vero e proprio furto di identità a danno di altri individui, in quanto le generalità inserite nel documento sono spesso indicate a caso e quasi mai corrispondono ad una persona realmente esistente. Lo scopo è evidentemente quello di non comparire

5 Tale metodo viene adottato dalle banche online proprio per contrastare e prevenire i casi di conti correnti attivati con furto di identità, ma è una procedura evidentemente ancora insufficiente e che andrebbe sicuramente perfezionata con maggiori e più stringenti controlli degli istituti bancari e postali.

in prima persona nel caso gli accertamenti degli inquirenti risalgano al rapporto bancario/postale utilizzato per la truffa, o comunque quello di cercare di allontanare le prove a proprio carico, fingendo di essere egli stesso vittima di furto di identità o dell'uso fraudolento del proprio documento. In tale contesto si verificano spesso casi in cui il truffatore utilizza il proprio documento senza falsificarlo, ma presentando comunque in precedenza una finta denuncia di furto o di smarrimento. In questo modo il responsabile ritiene di essere al sicuro fingendo di non essere più in possesso del proprio documento di identità. In realtà però, si tratta di un maldestro tentativo di farla franca perché, per poter utilizzare il proprio documento, questo deve inevitabilmente riportare una fotografia con la propria effige, il che esclude qualsiasi utilizzo del documento fatto da altri[6].

d. Conto corrente e/o carta di credito ricaricabile attivato regolarmente da altra persona consapevole.
Le truffe sono portate a termine attraverso i pagamenti delle vittime effettuati su un conto corrente (o su carta di credito) regolarmente attivato da altra persona e ad essa intestato (generalmente un parente o un amico o un fidanzato) di cui il truffatore ha la disponibilità. In questo caso è possibile che l'intestatario del rapporto bancario sia consapevole dell'uso illecito che di esso viene fatto, ovvero sia all'oscuro delle truffe che con esso vengono commesse, ferme restando le sue responsabilità, perlomeno morali, nel mantenere attivo un conto corrente di cui ha la piena titolarità, senza controllarne le movimentazioni. In questi casi l'attività del truffatore è sicuramente meno complicata non dovendo preoccuparsi di carpire illecitamente i dati e i documenti di altre persone.

e. Conto corrente e/o carta di credito ricaricabile attivato regolarmente da altra persona inconsapevole.
In questo caso l'intestatario del rapporto bancario è totalmente inconsapevole dell'uso illecito che di esso viene fatto, dal momento che – a differenza della ipotesi precedente – esso è vittima di una attività di *phishing* ai suoi danni (utilizzata per ottenere le credenziali di accesso online e, tramite esso, la disponibilità del conto/carte di credito ricaricabile).

f. Conto corrente e/o carta di credito attivato da prestanome.
Per portare a termine le truffe, il responsabile utilizza conti correnti o carte di credito di cui egli ha la piena disponibilità, ma che sono intestati ad altre persone le quali, in realtà, sono meri *prestanome* che vengono indotti ad attivare tali conti e/o carte con minacce, inganni ovvero approfittando della loro situazione di indigenza. Si tratta generalmente di persone senza fissa dimora, che vivono ai margini della società, a volte anche con problemi di salute mentale, che in cambio di pochi euro attivano tali rapporti bancari di cui poi però non hanno mai la reale

6 A meno che non venga accertata la complicità dell'operatore bancario o postale, che comunque non è da escludere a priori.

disponibilità in quanto le credenziali di accesso vengono immediatamente cedute ai truffatori.

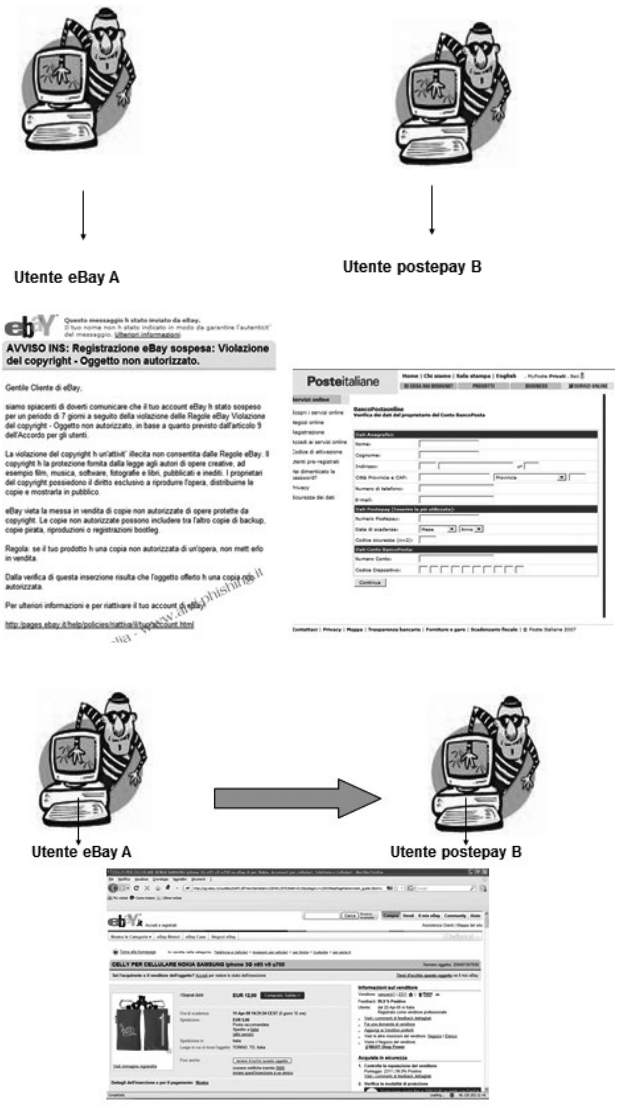
g. Utenze telefoniche intestate ad altre persone.
Con i medesimi documenti falsificati, il truffatore generalmente attiva varie utenze telefoniche mobili che quindi risultano intestate ad altre persone. Tali utenze sono utilizzate dal responsabile per mantenere i contatti con le vittime delle sue truffe fino a quando queste non abbiano provveduto al pagamento. Nella quasi totalità dei casi infatti, dopo il primo contatto che le parti hanno attraverso il sito web e attraverso i rispettivi *account* di posta elettronica, la fase di contrattazione avviene generalmente attraverso il mezzo del telefono.
Oltre che con documenti falsificati, l'utenza telefonica utilizzata per le truffe viene spesso attivata anche con documenti regolari da persone, generalmente straniere e difficilmente reperibili perché senza fissa dimora sul territorio nazionale, le quali poi la consegnano al truffatore in cambio di pochi euro.

h. Connessioni internet effettuate attraverso computer violati.
I collegamenti internet eseguiti per effettuare le registrazioni presso i siti di *e–commerce*, ovvero per inserire gli annunci delle false vendite, ovvero per creare gli *account* di posta elettronica e utilizzarli poi durante la fase della contrattazione, sono realizzati attraverso computer violati ovvero controllati dai reali truffatori all'insaputa dei proprietari, per carenza di protezioni antivirus. In tali casi l'utenza telefonica che è collegata alla rete internet risulta intestata a persone completamente ignare dell'uso illecito che viene fatto del proprio computer e della propria linea internet. È evidente che questo tipo di attività richiede conoscenze tecniche e informatiche molto avanzate; essa viene posta in essere soprattutto nei casi di truffe su piattaforme di *e–commerce* commesse da singoli truffatori che sono anche notevolmente esperti in materia informatica, ovvero dalle organizzazioni criminali che reclutano tali individui affidando loro esclusivamente il compito di garantire una connessione telematica sicura e difficilmente rintracciabile dagli organi inquirenti.

Questi dunque sono i principali esempi di truffe commesse tramite sostituzione di persona, rilevati nel corso degli ultimi anni (dei quali peraltro si è già parzialmente fatto cenno nelle considerazioni del precedente paragrafo): essi tuttavia non devono essere considerati in modo circoscritto e definitivo, in quanto spesso i rei hanno portato a termine truffe di questo tipo utilizzando contemporaneamente anche due o più modalità sopra descritte. È questo il "caso di scuola" di truffe realizzate abbinando il meccanismo descritto sub a. ed e. (tramite invio di *e–mail* di *phishing* volte ad acquisire una falsa identità sia lato venditore sia lato titolare del rapporto bancario beneficiario del pagamento) e qui sotto illustrato a livello di immagini:

TRUFFE SU PIATTAFORME DI E-COMMERCE TRAMITE SOSTITUZIONE DI PERSONA

Figura 1.



Appare così evidente che, a fronte di un siffatto articolato *modus operandi*, le investigazioni non faranno altro, quantomeno in prima battuta, che individuare i titolari (utenti A e B) quali vittime di *phishing*. Le somme di denaro, di regola, non saranno comunque recuperabili in quanto il truffatore, dopo averle fatte confluire sulla postepay di cui ha ottenuto indebitamente la disponibilità, ugualmente – tramite operazioni online – le indirizzerà verso altre carte a lui comunque riconducili, ponendole prontamente poi all'incasso.

3. LE SOLUZIONI ORGANIZZATIVE APPRONTATE PER FAR EMERGERE PROFILI DI SERIALITÀ [GENNAIO 2008–MAGGIO 2015] E TUTELARE LE VITTIME

L' illustrazione delle caratteristiche del fenomeno illecito oggetto di analisi fa emergere con evidenza la necessità di affiancare al metodo investigativo un metodo organizzativo ugualmente efficiente ed efficace per il contrasto di tali reati.

3.1 La concentrazione di tutti i fascicoli in capo ad un unico Pubblico Ministero

In tale ottica quindi, nel gennaio del 2008, l'allora Procuratore della Repubblica presso il Tribunale di Milano Manlio Minale, preso atto della "*opportunità di concentrare i procedimenti relativi ad ipotesi di truffa tramite internet nell'ottica dell'opportuna omogeneità di valutazione e del necessario coordinamento delle indagini, anche al fine di individuare le ipotesi seriali*", di intesa con il Procuratore Aggiunto Alberto Nobili (all'epoca coordinatore del VII Dipartimento, all'interno del quale era ricompreso il pool reati informatici) disponeva in tal senso con apposita circolare interna. Già da tempo, infatti, era stato rilevato un significativo aumento di tale tipologia di reati, meritevole di una trattazione non solo unitaria ma anche ad opera dei magistrati già organizzati nel richiamato pool, al fine di rendere più efficace ed incisiva la risposta investigativa (anche nel raccordo con le forze di Polizia specializzate sul territorio nonché con la Squadra reati informatici della Procura, costituitasi nel maggio 2007). Per l'effetto di tale disposizione interna, che di fatto ha comportato la concentrazione di tali reati in capo ad un unico Pubblico Ministero, nel periodo intercorso tra gennaio 2008 e maggio 2015 sono stati trattati unitariamente 12.640 fascicoli (pari ad una tendenza media di 1723 fascicoli per anno), così suddivisi:

mod. 21 – **3.689**
mod. 44 – **8.951**

totale **12.640**

Un significativo flusso, nuovamente aumentato[7] negli ultimi anni, alla stessa stregua dei *computer crimes*, come attestato dai seguenti dati:

5 aprile 2007 – 4 aprile 2008: 630
5 aprile 2008 – 4 aprile 2009[8]*:* **1653** *+ 162%*

1 luglio 2012 – 30 giugno 2013[9]*: 971*
1 luglio 2013 – 30 giugno 2014[10]*:* **2012** *+ 107%*

1 luglio 2014 – 30 giugno 2015[11]*:* **2530** *+ 26%*

Per rendere maggiormente efficace l'azione di contrasto, a partire dal 2009 – grazie anche all'apporto del Criminologo distaccato dal Comune di Milano a seguito della *partnership* con il pool reati informatici[12] – è stato elaborato un *database* interno in grado di evidenziare elementi di serialità nella commissione di tali fatti reato.
Tale *database* è stato alimentato per alcuni anni, giusti accordi intercorsi con l'Università Bicocca, da alcuni studenti universitari quanto ai fascicoli relativi agli anni 2010 e 2011 (si vedano anche alcuni saggi accademici pubblicati[13]).
Questa prima sperimentazione ha consentito di individuare e far emergere degli elementi ricorrenti tra fascicoli apparentemente riferibili a situazioni non omogenee.
Oltre al *database* (utilizzato soprattutto nei primi anni), la concentrazione dei fascicoli a carico di un solo Pubblico Ministero della Procura di Milano ha consentito – avvalendosi di *report* aggiornati quadrimestralmente – di raggruppare i fascicoli dai quali emergono profili di serialità.
In tale contesto vengono anche richiamati, per connessione interna, eventuali altri fascicoli processuali a carico dello stesso truffatore, ove ancora pendenti presso altri Pubblici Ministeri della Procura[14]; ciò

7 Dopo una anomala diminuzione nel 2010/2011.
8 Si veda sul punto F. CAJANI, *Considerazioni sull'impatto della "distrettualizzazione" ex legge 48/2008 sul pool reati informatici della Procura di Milano*, in AA.VV, (a cura di G. COSTABILE, A. ATTANASIO), *IISFA Memberbook 2100 Digital Forensics*, Forlì, 2010 – reperibile anche a partire da *www.procura.milano.giustizia.it/files/F-CAJANI-Brevi-considerazioni-impatto-legge-48.pdf.*
9 Fonte: Bilancio di responsabilità sociale 2012–2013.
10 Fonte: Bilancio di responsabilità sociale 2014–2015.
11 Fonte: Bilancio di responsabilità sociale 2014–2015.
12 Cfr. A.BERSINO, F.CAJANI,W. VANNINI (a cura di), *Presentazione delle linee guida concordate tra Procura della Repubblica, Ordine forense e Comune di Milano per ridurre il danno da reati informatici e tutelare le vittime*, reperibile a partire *da www.procura.milano.giustizia.it/files/PRESENTAZIONE-DELLE-LINEE-GUIDA-PER-RIDURRE-IL-DANNO-DA-REATI-INFORMATICI-E-TUTELARE-LE-VITTIME-Milano-10-ottobre-2014-_-DEF.pdf.*
13 Quanto ai fascicoli del 2010 cfr. C. PECORELLA, *Truffe on-line: momento consumativo e competenza territoriale, www.penalecontemporaneo.it/upload/1336549542pecorella.pdf*; Quanto invece all'analisi dei fascicoli del 2001 cfr. C.PECORELLA, M.DOVA, *Profili penali delle truffe on-line, www.archiviopenale.it/apw/wp-content/uploads/2013/09/Confronto.Pecorella.Dova_.pdf.*
14 Può infatti capitare, perché magari iscritto con qualificazioni giuridiche differenti dal 640 c.p., che alcuni fascicoli sfuggano alla attività di "concentrazione" sopra descritta.

consentirà evidentemente di esercitare l'azione penale in modo unitario per tutte le truffe attribuite alla stessa persona, evitando in questo modo (o per lo meno riducendo) sia la duplicazione delle indagini, sia la moltiplicazione di processi a carico dello stesso imputato (che potrà pertanto essere giudicato in un unico processo per tutte le truffe di cui viene accusato), con inevitabili ripercussioni positive anche sui costi sostenuti per l'esercizio dell'azione penale, sia nella fase requirente, sia nella fase giudicante.
Con una stima ragionevole alla luce della pregressa esperienza, la media per ogni truffatore seriale si attesta sui 10/15 fascicoli (e relative, conseguenti, persone offese).

3.2 Le Direttive per la Polizia Giudiziaria e l'attenzione verso la vittima

Vittime delle truffe su piattaforma di *e–commerce* risultano essere persone di tutte le età: l'analisi fatta sui fascicoli del 2010 aveva attestato che le percentuali maggiori si registravano tra quelle di età compresa tra i 35 e i 44 anni (circa il 28%) e tra 25 e i 34 anni (circa il 27%); decisamente inferiore era il numero dei più giovani, tra i 18 e i 24 anni (circa il 13%), nonché quello delle persone che hanno superato i 55 anni di età (circa il 9%)[15].
L'entità del danno patrimoniale subito, nel singolo caso, non è particolarmente elevato: sempre l'analisi dei fascicoli del 2010 e del 2011 aveva attestato che in prevalenza era in misura non superiore ai 300,00 euro.
Eppure, nonostante questo, indubbiamente si tratta di fatti di reato pericolosi perché suggestivi di prassi criminali facili: attività illecita, ma incruenta e ripetibile, la truffa a mezzo computer è capace di notevoli flussi economici, *"(...) pur mantenendo il dono dell'immaterialità, esperienza di cui non andrebbe sottovalutata la componente per più versi seduttiva, della distanza (di luogo e di tempo) dal fatto, e dalla virtuale (ahimè concreta) vittima"*[16].
Ed infatti, dal punto di vista criminale, è ovvio che l'uso del computer a fini malevoli venga percepito come intrinsecamente più sicuro di altri atti illeciti: un'attività emulabile con minime difficoltà tecniche e minimo bagaglio di cultura generale. Dunque attività presto virale, pervasiva, evidente incentivo a superare ogni incertezza per attori in grado di realizzare l'impresa. E di ciò consapevoli.
In altre parole, *"l'informatica malevolmente utilizzata sembra permettere la realizzazione dello scopo lucrativo in un tempo rappreso, idealmente istantaneo, in sincrono con più vittime e contemporaneamente in luoghi tra loro lontani, in costanza di un relazione vittima/autore di reato indifferente ad ogni distanza, se non per gli effetti positivi del distanziamento e delle molte relazioni contemporanee che è possibile realizzare. Tanto la truffa tradizionale richiede la collaborazione attiva*

15 Cfr. nota precedente.
16 E. PANZETTI, "*Note sulla psicologia della vittima e dell'incorporeità*", paper non pubblicato, Comune di Milano, ottobre 2011

della vittima, tanto la risorsa informatica permette di avere collaborazione attiva senza la necessaria frequentazione fisica; tanto il truffatore tradizionale deve ricorrere ad un arsenale concreto di apparenze e raggiri, tanto il truffatore informatico agisce l'adeguatezza relazionale – secondo stilemi attesi – e fisica – assecondanti stereotipi correnti – con maggiori gradi di creatività e di libertà, minor rischio e maggiore appagamento narcisistico ed economico"[17].

Anche tenendo in mente siffatte considerazioni, nel maggio del 2011 si è arrivati - a cura di un gruppo di lavoro in seno al pool reati informatici della Procura di Milano – alla formalizzazione (e alla successiva diffusione sotto forma di Direttive[18]) di vere e proprie procedure investigative *"sui primi accertamenti di Polizia Giudiziaria in materia di reati informatici"* nonché di alcune indicazioni operative sulle *"modalità di trasmissione delle relative comunicazioni di notizia di reato alla Procura della Repubblica di Milano"*.

Contestualmente alla redazione di tale documento e partendo dall'evidenza che l'operatore di Polizia Giudiziaria è spesso il primo rappresentante delle istituzioni con cui la vittima riesce ad entrare in contatto, è stata poi affrontata la questione di come costruire la migliore relazione possibile con la vittima.

Vittima che, nella più parte dei casi, è in condizione di trauma. Non importa quanto al professionista, all'Ufficiale di Polizia, appaia comune l'esperienza che gli viene raccontata, quanto possa suonare ripetizione di centinaia di altre e uguali: dal punto di vista di chi ha subito, la prospettiva è differente, la violenza subita, fosse anche una truffa, non è mai ordinaria.

Si è riflettuto pertanto sulla importanza professionale, anche per puro interesse investigativo, dei primi contatti con la vittima.

La possibilità di avere tempestivamente informazioni è un elemento essenziale, specie nella imminenza dell'accaduto. Avere informazioni il più possibile esaurienti di quanto accaduto significa che il nostro interlocutore non dovrebbe essere emozionato, annichilito, confuso, amareggiato o uno dei molti vissuti di chi ha subito un torto. Ma chi siede davanti all'Ufficiale di PG che raccoglie la testimonianza, la querela o la denuncia, è esattamente in tali condizioni.

Così, nelle Direttive, in modo forse poco articolato, si incentiva all'attenzione, all'accoglienza e a non sottovalutare il dato esistenziale. Non sottovalutare significa comprendere innanzitutto il punto di vista emotivo della vittima, del suo sentirsi traumatizzato. Ricordando che per la vittima il trauma subito può essere ben più severo di quanto il fatto in sé farebbe pensare.

Entrare in relazione è comprendere il punto di vista di costui o costei, secon-

17 Così W.VANNINI (con F.CAJANI e D. AGOSTINO), *"Di necessità, virtù": appunti per una strategia globale al contrasto del cybercrime. L'esperienza del pool reati informatici della Procura di Milano, in IISFA Memberbook 2011* (a cura di G. COSTABILE, A. ATTANASIO), Experta, 2012.

18 La nota del Procuratore di Milano Edmondo Bruti Liberati, che accompagna il testo delle direttive, è reperibile all'indirizzo *www.procura.milano.giustizia.it/files/prime-pagine-da-direttive-per-la-polizia-giudiziar.pdf*.

do l'età, la cultura, il genere, e le molte variabili note all'operante di PG[19]. E dunque le Direttive, quanto alla tipologia di reati informatici che qui ci occupa, prevedono altresì che la Polizia Giudiziaria, in sede di ricezione della denuncia querela, debba richiedere alla persona offesa le seguenti informazioni (utili al proseguo delle indagini, in quanto la complessità e la durata di tutta l'attività di indagine potranno essere tanto più ridotte quanto più numerose saranno le informazioni che la vittima è in grado di riferire):

a) su quale sito di vendita online è avvenuto il primo contatto con il truffatore, con quale nickname questi appariva registrato, l'eventuale codice che contrassegnava l'offerta di vendita.

b) con quale *account* di posta elettronica il presunto venditore ha portato avanti la contrattazione, non omettendo di allegare la stampa di tutte le *e–mail* inviate e ricevute (comprensive di *header*[20]), indicando altresì su quale *account* di posta elettronica la vittima ha eventualmente trasmesso la copia dei propri documenti di identità, se diverso dal precedente;

c) nel caso ci siano stati anche contatti telefonici, quale utenza il truffatore ha utilizzato, precisando inoltre se la persona che ha mantenuto i contatti fosse un uomo o una donna, se la sua voce avesse accenti particolari, sia italiani, sia stranieri;

d) in che modo è avvenuto il passaggio di denaro a favore del truffatore, indicando con precisione il luogo, la data, l'ora e ogni altra circostanza in cui esso è avvenuto;

e) ogni possibile riferimento che contraddistingue il titolo di pagamento verso il quale i soldi sono stati trasmessi (codice IBAN[21] del conto corrente, numero di carta di credito prepagata, numero di vaglia postale, etc.);

---

19 Naturalmente le Direttive, pensate come manuale strettamente operativo funzionale alla veloce e corretta definizione del fatto e delle procedure cogenti da porre in essere, potevano solo invitare all'attenzione, rimandando ad altre fonti una più articolata riflessione. Anche da qui è nato poi il corso di formazione per la PG online e in presenza che si è concluso lo scorso anno (e che verrà rieditato a breve) e l'esperienza di un workshop sperimentale di formazione alla accoglienza della vittima in condizioni di trauma. Workshop che probabilmente anch'esso verrà ripetutonel 2016: cfr. sul punto nota 12

20 Trattasi delle informazioni di una *e–mail* presenti nel suo formato digitale, e che possono essere in ogni caso stampate dal destinatario tramite una procedura ad hoc.

21 L'IBAN (*International Bank Account Number*) è un codice composto da 27 caratteri che identifica in modo univoco un conto corrente:
– 2 lettere rappresentanti il Paese (IT per l'Italia);
– 2 cifre di controllo, ossia il CIN EUR;
– il codice BBAN nazionale (CIN + ABI + CAB + Numero di conto).
Tramite numerosissimi siti internet è possibile identificare la filiale di appartenenza di un determinato conto corrente (del quale si è in possesso del numero IBAN o, comunque, almeno dei seguenti dati:
– codice ABI (Associazione Bancaria Italiana), numero composto da cinque cifre e rappresenta l'istituto di credito;
– codice CAB (Codice di Avviamento Bancario), numero composto da cinque cifre e rappresenta l'agenzia o specifica filiale dell'istituto di credito identificato dal codice ABI.

f) nel caso in cui ci siano stati anche incontri con i presunti venditori, la descrizione precisa delle persone incontrate, non omettendo di indicare il luogo, la data, l'ora e ogni altra circostanza in cui tali incontri si sono verificati.

4. IL PROBLEMA DEI CRITERI DI INDIVIDUAZIONE DELLA COMPETENZA TERRITORIALE

Fino alle prime prese di posizione, nel 2008, della Procura Generale presso la Corte di Cassazione in sede di risoluzione dei contrasti negativi di competenza *ex* art. 54 c.p.p., il criterio tradizionalmente seguito da molti Uffici Giudiziari requirenti era quello del luogo di conseguimento dell'illecito profitto, da identificarsi nel luogo di apertura del conto corrente (o di altro mezzo di pagamento quale una carta postepay) indicato dal venditore al compratore ovvero quello residuale *ex* art. 9 comma 2 c.p.p. (luogo di residenza/dimora/domicilio dell'indagato).
Tale impostazione, oltre che basarsi su dati immediatamente presenti nei fascicoli processuali, portava con sé un dato di esperienza investigativa che non deve essere dimenticato e al quale abbiamo già fatto cenno al paragrafo precedente: infatti, in relazione a tale tipologia di reato (ove il discrimine con una controversia civilistica ricollegabile al mero inadempimento della controprestazione dell'invio del bene venduto è sempre, *ab origine*, di sottile percezione) solo una "concentrazione" di fascicoli presso le Procure così organizzate è in grado di far apparire immediatamente se trattasi di mero episodio sporadico e se invero si è in presenza di veri e propri truffatori seriali.

4.1 L'iniziale impostazione della Procura Generale presso la Corte di Cassazione (con riferimento ai pagamenti verso carte postepay)

Per quanto sopra indicato una simile "concentrazione" può dunque realizzarsi solamente ove venga individuato un criterio di competenza che prescinda da altre circostanze verificatesi nel caso concreto, quali invece quelle valorizzate dall'orientamento seguito dalla Procura Generale presso la Corte di Cassazione a partire dal decreto del 24.1.2008[22]:

"il reato di truffa è un reato istantaneo e di danno, che si realizza al momento della effettiva prestazione del bene economico da parte del soggetto raggirato, con il correlativo arricchimento dell'agente;
[..] nel caso in esame, la deminutio patrimonii del soggetto passivo si realizza nel momento in cui lo stesso compie l'operazione di ricarica della carta postepay [...] presso l'Ufficio postale di Moggio Udinese;
[..] contestualmente, con la disponibilità cioè sulla carta di cui è in possesso, della somma versata si verifica l'ingiusto profitto dell'agente, a

22 Nr. 20/2A/2008 PG – 28/08 R.D.

prescindere dal luogo in cui la somma viene effettivamente riscossa, giacché l'arricchimento è costituito dalla mera disponibilità e non già dall'effettiva spesa o prelievo della somma; [...] pertanto il luogo di consumazione va individuato in Moggio Udinese".

Tale impostazione è stata così massimata[23]:

"In caso di truffa commessa ricaricando una carta Poste Pay, la deminutio patrimonii del soggetto passivo si realizza nel momento in cui viene compiuta l'operazione di ricarica, e quindi nel luogo in cui ha sede l'ufficio postale utilizzato; contestualmente con la disponibilità sulla carta della somma versata si verifica l'ingiusto profitto dell'agente a prescindere dal luogo in cui la somma viene effettivamente riscossa, giacchè l'arricchimento è costituito dalla mera disponibilità, non già dell'effettiva spesa o prelievo della somma".

L'argomentazione in diritto sopra richiamata sembra fare riferimento alla nota sentenza delle Sezioni Unite, 1 agosto 2000, n. 18[24], così massimata:

"Poiché la truffa è reato istantaneo e di danno, che si perfeziona nel momento in cui alla realizzazione della condotta tipica da parte dell'autore abbia fatto seguito la "deminutio patrimonii" del soggetto passivo, nell'ipotesi di truffa contrattuale il reato si consuma non già quando il soggetto passivo assume, per effetto di artifici o raggiri, l'obbligazione della "datio" di un bene economico, ma nel momento in cui si realizza l'effettivo conseguimento del bene da parte dell'agente e la definitiva perdita dello stesso da parte del raggirato. Ne consegue che, qualora l'oggetto materiale del reato sia costituito da titoli di credito, il momento della sua consumazione è quello dell'acquisizione da parte dell'autore del reato, della relativa valuta, attraverso la loro riscossione o utilizzazione, poiché solo per mezzo di queste si concreta il vantaggio patrimoniale dell'agente e nel contempo diviene definitiva la potenziale lesione del patrimonio della parte offesa".

Impostazione peraltro ripresa anche da Cass., Sez. V, 6 aprile 2009, n. 14905[25], così massimata:

"Ai fini della consumazione del reato di truffa è necessario che il profitto dell'azione truffaldina entri nella sfera giuridica di disponibilità dell'agente, non essendo sufficiente che esso sia fuoriuscito da quella del soggetto passivo".

23 cfr. sinossi relativa ai decreti adottati nel 2008, di cui alla nota prot. 16253/SP Procura Generale presso la Corte Suprema di Cassazione del 14.10.2008.
24 in *CED 216429*.
25 in *CED 243608*.

4.2 Un primo mutamento della Procura Generale in relazione alle ipotesi di pagamenti tramiti bonifici su conti correnti

La stessa Procura Generale presso la Corte di Cassazione – su sollecitazione della Procura di Milano – intervenne però successivamente per individuare la regola di competenza nel diverso caso (non preso in considerazione nel provvedimento del 2008) di pagamento effettuato dalla persona offesa tramite bonifico bancario a favore del conto corrente del venditore[26]. Così infatti il provvedimento datato 29.10.2009[27]:

Che, invero il reato di truffa – come reato istantaneo e di danno – si perfeziona, secondo il costante orientamento giurisprudenziale della Corte Suprema (Cass. Sez. Un., ud. 16.12.1998, dep. 19.1.1999, n. 1, Cellammare, in C.E.D., rv.: 212080, e in Cass. pen., 1999, p. 1415, m. 640; Cass. Sez. Un., C.c. 21.6.2000, dep. 1.8.2000 n.18, Franzo ed altri, in C.E.D., rv.: 216429, e in Cass. pen., 2000, p. 3270, m. 1764), nel luogo del conseguimento dell'effettivo profitto, con il contestuale concreto danno patrimoniale subito dalla parte offesa;

Che è giurisprudenza costante della Suprema Corte che, nell'ipotesi di truffa cosiddetta "truffa contrattuale" il reato si consuma – stante appunto la sua natura di reato istantaneo e di danno – non già quando il soggetto passivo assume, per effetto di artifici o raggiri, l'obbligazione della dazione di un bene economico, ma nel momento in cui si verifica l'effettivo conseguimento del bene da parte dell'agente e la definitiva perdita dello stesso da parte del raggirato e che, pertanto, nel caso in cui la truffa si realizzi con la stipulazione di un negozio giuridico con effetti obbligatori, il profitto ed il danno si identificano nell'esecuzione della prestazione pattuita (in tal senso, Cass. Sez. I, C.c. 26.2.1973, dep 6.6.1973, n. 431, Gianni, in C.E.D., rv.: 124244; Cass. Sez. II, ud. 4.02.2002, n. 25193, dep. 2.07.2002, Bari, in C.E.D., rv.: 222124) e il reato si perfeziona dove e quando il soggetto passivo subisca la definitiva perdita del bene economico, che entra nella disponibilità immediata dell'autore del reato (Cass. Sez. II, ud. 11.07.2008, n. 31044, dep. 24.07.2008, Miano, in C.E.D., rv.: 240659);

Che, infatti, in tema di titoli di credito, si afferma costantemente il principio secondo cui "Quando il reato predetto abbia come oggetto immediato il conseguimento di assegni bancari, il danno si verifica nel momento in cui i titoli vengono posti all'incasso, ovvero usati come normali mezzi di pagamento, mediante girata a favore di terzi portatori legittimi" (Cass. Sez. II, ud. 24.1.2002, dep. 8.7.2003, n. 28928, Miglio-rini, in C.E.D., rv.: 226745; Cass. Sez. II, ud. 28.10.1997, n. 1136, dep.

26 In questi casi di regola è immediatamente possibile risalire alla banca interessata laddove sia indicato dalla persona offesa il codice IBAN di tale istituto beneficiario.

27 N. 241/2A/ 2009 Reg. P.G. – 254/09 R.D. (est. Passacantando).

29.01.1998, Stabile, in C.E.D., rv: 209671; Cass. Sez. VI, ud. 24.05.2000, n. 10539, dep.10.10..2000, Marcoccia, in C.E.D., rv.: 217308);

Che, pertanto, nel caso di specie, l'acquisto del bene da parte del soggetto passivo è avvenuto a mezzo di bonifico bancario sul c/c Poste Italiane in Modena intestato ai due sopra menzionati indagati, e, quindi, l'effettivo conseguimento dell'ingiusto profitto da parte degli agenti, con la conseguente concreta e definitiva perdita del bene subita dalla parte offesa, è avvenuto soltanto in Modena con l'accreditamento della somma e il positivo esito del disposto bonifico bancario sul c/o predetto in favore del [...] (e quindi con modalità di tempo e di luogo diverse – agli effetti della definitiva diminuzione patrimoniale subita dal soggetto passivo e dell'incremento economico ingiusto acquisito dal soggetto attivo – da quelle seguite con il pagamento effettuato con la ricarica delle carte prepagate);

In tali ipotesi si era quindi ritornati ad applicare i criteri tradizionalmente seguiti da molte Procure già prima del 2008.

4.3 Il successivo orientamento della Procura Generale in relazione alle ipotesi di pagamenti tramite carte di credito ricaricabili e alle c.d. banche online

Orbene nel 2013 la Procura Generale presso la Corte di Cassazione, mutando il suo originario orientamento del 2008, ha finito di applicare gli stessi principi di cui al richiamato provvedimento del 2008 anche nelle ipotesi di pagamenti tramite carte postepay.
Più precisamente (cfr. ex pluribus decreto n. 44/2013[28]), partendo dalle medesime premesse alla base del precedente orientamento[29], le deduzioni argomentative finali ora sono le seguenti:

Tale momento (consumativo: n.d.a.) andrebbe comunque individuato laddove sia in considerazione una truffa contrattuale ricollegabile a offerta pubblicata su sito internet non (solo) nell'operazione di ricarica posta in essere dalla persona offesa ma nella conseguente effettiva provvista di valuta mediante l'accredito "indirizzato" di una somma di danaro quale corrispettivo per il bene offerto in vendita attraverso uno strumento di pagamento (la carta prepagata) convenuto contrat-

28 Est. Corasaniti.

29 *"La S.C. (Sez. 2, Sentenza n. 18859 del 24/01/2012) ha recentemente affermato, proprio con riferimento all' ipotesi di truffa contrattuale come la truffa è reato istantaneo e di danno, che si perfeziona nel momento in cui alla realizzazione della condotta tipica da parte dell'autore abbia fatto seguito la* "deminutio patrimonii" *del soggetto passivo: ne consegue che, nell'ipotesi di c.d. truffa contrattuale, il reato si consuma non già quando il soggetto passivo assume, per effetto di artifici o raggiri, l'obbligazione della "datio" di un bene economico, ma nel momento in cui si realizza* l'effettivo conseguimento del bene da parte dell'agente e la definitiva perdita dello stesso da parte del raggirato.
L'indirizzo giurisprudenziale in tema di truffa contrattuale si palesa del resto in qualche modo uniforme, che poi si ricollega alla valutazione del mezzo di pagamento del corrispettivo di volta in volta utilizzato

tualmente e cioè mediante indicazione del relativo codice univoco, qualificandosi peraltro come vero e proprio "domicilio informatico" del creditore apparente ai sensi e per gli effetti degli artt. 1182 e 1498 comma 3 del codice civile.

Pertanto, come poi ripreso in altri provvedimenti del 2014 (cfr. ex pluribus n. 223/2014[30]):

- la truffa contrattuale è reato istantaneo e di danno;
- irrilevante ove il raggirato abbia provveduto – mediante "accredito indirizzato" del corrispettivo in denaro all'acquisito – alla "ricarica", detta truffa si consuma con l'acquisizione da parte dell'autore del reato delle della provvista
- assume dunque rilievo, ai sensi e per i fini di cui all'art. 8 c.p.p., il luogo ove è stata attivata la carta prepagata e si trova il "conto" ad essa collegato, identificabile tramite il relativo "codice univoco" e qualificabile come vero e proprio "domicilio informatico" dell'apparente creditore, indagato quale truffatore.

Tale mutato orientamento, nelle stesse parole della Procura Generale della Corte di Cassazione:

ha peraltro il pregio di consentire – nel caso in cui all'annuncio "truffaldino" abbiano aderito più utenti di internet delle più disparate parti d'Italia – il quanto più possibile sollecito confluire di tutte le notizie criminis presso un unico ufficio di Procura.

Alla luce di tale impostazione sempre la Procura Generale presso la Corte di Cassazione ha precisato che ove poi tali pagamenti, a mezzo di bonifico della persona offesa, vengano effettuati a favore delle cd. banche *online* occorrerà ricorrere ai criteri di cui al secondo comma dell'art. 9 c.p.p.[31]

(Sez. 2, Sentenza n. 20025 del 13/04/2011, Sez. 2, Sentenza n. 43347 del 1511012009, Sez. 2, Sentenza n. 36502 del 17/06/2009, Sez. 2, Sentenza n. 31044 del 11/0712008, Sez. 2, Sentenza n. 25193 del 04/02/2002) . È bene rilevare inoltre come il reato di truffa si consuma nel momento dell'effettivo conseguimento dell'ingiusto profitto, con correlativo danno della persona offesa, corrispondente al momento dell'effettiva prestazione del bene economico da parte della vittima, con conseguente passaggio nella sfera di disponibilità del reo (Sez. 2, Sentenza n. 42958 del 18/11/2010). Il reato di truffa si perfezionerebbe,perciò, in casi analoghi nel momento in cui alla realizzazione della condotta tipica abbiano fatto seguito la "deminutio patrimonii" del soggetto passivo e la "locupletatio" dell'agente, sicché, proprio come nell' ipotesi di pagamento del corrispettivo mediante assegni, il momento della sua consumazione è quello dell'acquisizione da parte dell1autore del reato, della relativa valuta, attraverso la loro riscossione o utilizzazione, essendo irrilevante, ai fini del vantaggio patrimoniale dell'agente, il momento della consegna dei titoli da parte del "deceptus" (Sez. 2, Sentenza n. 5428 del 22/0112010). E tale linea argomentativa trae origine dalla giurisprudenza delle sezioni unite (sentenza n. 18 del 21/06/2000) proprio in tema di truffa contrattuale".

30 Est. Romano.

31 Cfr. *ex pluribus* decreto 51/2014 (Est. Romano).

4.4 La recente sentenza della Corte di Cassazione, sez. I penale, n. 25230/2015[32]

In un siffatto contesto giurisprudenziale, che ormai sembrava consolidato e finalmente idoneo a sostenere l'azione delle Procure più sensibili a perseguire la serialità insita in tale tipologia di reato, è intervenuta di recente la Suprema Corte nel risolvere (qui non più un contrasto tra Procure bensì) un conflitto tra due Tribunali. Significativo riscontrare che, ancora una volta, le premesse sono identiche:

[...] In tema di truffa le Sezioni Unite penali di questa Corte hanno di recente ribadito che trattasi di reato istantaneo e di danno che si perfeziona nel momento in cui alla realizzazione della condotta tipica da parte dell' autore abbia fatto seguito la "deminutio patrimoni" del soggetto passivo (S.U. – 16.12.98, Cellammare, CED 212079).
La giurisprudenza di questa Corte, inoltre, è concorde nel ritenere che la truffa c.d. contrattuale, quale è quella per cui si procede, è un reato di danno che si consuma nel momento in cui si verifica l'effettivo conseguimento del bene da parte dell'agente e la definitiva perdita dello stesso da parte del raggirato (cfr. ex plurimis, sez. II – 29.01.98, Stabile, CED. 209671; sez. II – 16.04.97, Tassinari, CED 207831). Danno che non solo deve avere contenuto economico, ma deve consistere anche per il soggetto passivo in una lesione del bene tutelato, concreta ed effettiva, e non soltanto potenziale (S.U., 22.03.69, P.M. c/Carraro, Cass. pen. 1969, pag. 1023; S.U., 30.11.74, Forneris, Cass. pen. 1975, pag. 741.). Va, infatti, osservato che la truffa è un reato che prevede, come elementi costitutivi, due requisiti: il conseguimento dell'ingiusto profitto da parte dell'agente e il danno da parte del soggetto leso: solo quando entrambi questi due elementi si sono verificati, la truffa può dirsi consumata proprio perché la condotta ingannatrice (alla quale sono riconducibili causa/mente i due suddetti eventi) si è completamente realizzata.Nei casi tipici in cui l'oggetto materiale del reato è costituito da titoli di credito, il momento della sua consumazione è stato indicato in quello dell'acquisizione da parte dell'autore del reato, della relativa valuta, attraverso la loro riscossione o utilizzazione, poiché solo per mezzo di queste si concreta il vantaggio patrimoniale dell'agente e nel contempo diviene definitiva la potenziale lesione del patrimonio della parte offesa.

Ma il risultato del ragionamento giuridico ai fini della individuazione del *locus commissi delicti*, ancora una volta, cambia direzione:

Nel caso in esame, tuttavia, il raggiro è stato realizzato attraverso l'uso di una carta postepay ricaricabile che consente il versamento di denaro su una carta propria o di terzi. Il conseguimento del profitto da parte del soggetto truffatore si è verificato nel momento stesso in cui la parte offesa ha proceduto al versamento del denaro sulla carta ricaricabile

32 NRG 2014 45748, ud. 13/03/2015 – dep. 16/06/2015. In CED, Archivio sentenze penali, non massimata.

a lui intestata. Detto versamento ha infatti realizzato contestualmente l'effettivo conseguimento del bene da parte dell'agente, che ha avuto immediatamente a disposizione la somma versata, e la definitiva perdita dello stesso da parte del raggirato. La competenza territoriale va quindi radicata nel luogo ove è stato effettuato il versamento [...].

4.5 Considerazioni finali in punto di individuazione della competenza territoriale in relazione alle truffe su piattaforma di e–commerce

Occorre nuovamente[33] ribadire come l'orientamento ora ripreso anche dalla Corte di Cassazione nel caso di truffe contrattuali con pagamento mediante carte ricaricabili[34] (individuando il luogo di competenza in quello ove la persona offesa pone il essere l'atto di disposizione patrimoniale) fa esclusivamente riferimento – nella sua premessa concettuale – al dato temporale, ovvero al momento in cui il reato di truffa possa dirsi consumato.
Esso infatti sembra far discendere da una interpretazione giurisprudenziale in tema di *tempus commissi delicti* un principio giuridico *ipso facto* applicabile in tema di *locus commissi delicti*: più semplicemente, tale criterio attiene esclusivamente al *tempus commissi delicti* perché invece lo stesso, se correttamente analizzato nella sua logica conseguenziale, non è in grado di fornire una soluzione univoca in relazione al locus *commissi delicti*.
E questo per un motivo semplicissimo: se è vero che alla *deminutio patrimoni* del soggetto passivo si realizza *"contestualmente l'effettivo conseguimento del bene da parte dell'agente, che ha avuto immediatamente a disposizione la somma versata"*, ci troviamo necessariamente di fronte – a livello di ragionamento logico – a due luoghi, entrambi identificabili immediatamente perché, proprio a seguito dell'*immediatezza* con cui si verifica il trasferimento pecuniario dalla disponibilità di un soggetto all'altro, essi emergono alla realtà dei fatti *contestualmente*.
E quindi, dall'analisi dei primi atti costituenti la comunicazione di notizia di reato, di regola non solo è possibile identificare l'ufficio postale ove la persona offesa abbia effettuato l'atto dispositivo (tramite ricarica postepay) ma anche l'ufficio ove l'indagato abbia attivato la carta postepay[35].
O, allo stesso modo nei casi di pagamento tramite bonifico bancario, nell'ufficio ove l'indagato abbia aperto il conto corrente beneficiario.
Che i luoghi pertanto siano due (o non già uno, come nelle ipotesi tra-

33 Cfr. F. CAJANI, *Aspetti giuridici comuni delle indagini informatiche – Competenza*, in AA.VV., *Computer Forensics e Indagini Digitali. Manuale Tecnico–Giuridico e Casi Pratici*, I, p. 197, Experta, 2011.

34 Si noti come, dalla lettura della sentenza, non è possibile comprendere se trattasi di postepay abbinata o meno ad un conto corrente.

35 La cui numerazione in questi casi viene sempre indicata nella denuncia, perché dato conosciuto dalla persona offesa in quanto a lei preventivamente comunicato dall'indagato: è pertanto immediatamente possibile – tramite richiesta a Poste Italiane (o anche usufruendo di un sistema di interrogazione *web based* che lo stesso istituto citato ha messo a disposizione delle forze dell'Ordine) risalire al luogo di apertura della stessa ad opera dell'indagato.

dizionali di truffa) deriva dalla natura stessa della tipologia del reato di cui ci stiamo occupando, dove – per definizione – in assenza di un contatto fisico le somme di denaro "non passano di mano" in un unico, oltre che ben definito, contesto spazio–temporale. Peraltro, in termini strettamente tecnico–operativi, la pretesa di poter individuare con esattezza il luogo ove la persona offesa effettua "la ricarica" o quello dove l'indagato la riceve, conseguendone così il profitto, viene meno nel caso più frequente di carta postepay non abbinata ad un conto corrente: ed infatti risulta una mera finzione identificare tali luoghi presso gli Uffici postali che vengono di volta in volta in rilievo, dal momento che tale tipo di pagamento può essere fatto ovunque anche tramite qualsiasi dispositivo elettronico (anche mobile) e il relativo incasso può avvenire presso qualsiasi ATM ugualmente dislocato sull'intero territorio nazionale[36]. Ne consegue pertanto che, a rigore, tale tipologia di reato (quantomeno nelle ipotesi di pagamento tramite ricarica postepay) rende *in re ipsa* inapplicabile il criterio *ex* art. 8 comma 1 c.p.p.

Continuare invece ad optare per il luogo del pagamento della persona offesa significa ancorare diversi procedimenti (tutti a carico del medesimo indagato) a criteri di competenza del tutto legati al mero caso. Ed arrivare per di più, in caso di ricarica di carta postepay abbinata ad un conto corrente, ad applicare un criterio diverso da quello applicabile – in ipotesi – nel caso di pagamento tramite bonifico bancario su analogo conto corrente. O, ancor peggio, introdurre nelle investigazioni su tale tipologia di reato una sorta di "spada di Damocle", relativa alla possibilità che la competenza – inizialmente radicatasi presso l'Ufficio requirente che ha ricevuto una CNR – possa ad un certo punto mutare laddove pervenga un'altra denuncia, relativa al medesimo indagato ma da parte di una persona offesa che abbia effettuato, *precedentemente*, un versamento in luogo *non rientrante* nel circondario di competenza di tale Procura (e pertanto, con la nascita di un nuovo procedimento a seguito di tale seconda CNR, i due fascicoli così riuniti dovrebbero essere trasmessi per competenza ad una diversa Procura. La quale paradossalmente, a sua volta, potrebbe continuare l'investigazione su quei due fatti ma ricevere una terza CNR riferibile al medesimo indagato ma con un pagamento,

36 Cfr. sul punto C.PECORELLA, M.DOVA, *Profili penali delle truffe on–line, cit*, i quali – pur riconoscendo la validità giuridica del criterio individuato fin dal 2008 dalla Procura Generale – tuttavia ritengono che tale criterio *"appare anche poco conforme alla ratio sottostante alla disciplina del codice di procedura penale nella quale si traduce la garanzia della precostituzione del giudice ai sensi dell'art. 25 co. 1 Cost.: secondo quanto dispone, come regola generale, l'art. 8 c.p.p., giudice 'naturale' del fatto è quello del locus commissi delicti perché la vicinanza con l'ambiente nel quale il reato si è realizzato dovrebbe rendere più agevole la raccolta delle prove e —si dice— consentire alla sentenza di condanna di svolgere al meglio la sua funzione dissuasiva. L'importanza di radicare la competenza del giudice penale nel luogo in cui opera il reo — anziché in quello in cui si trova la vittima — emerge d'altra parte chiaramente dall'analisi delle diverse regole dettate in materia dal codice di procedura penale". E così concludono come "vi siano valide ragioni per auspicare un intervento legislativo che, con riguardo ai reati che siano commessi a distanza, avvalendosi di un sistema informatico, individui la competenza territoriale del giudice attraverso un criterio diverso da quello incentrato sul luogo di consumazione del reato; soluzioni differenziate, del resto, sono state adottate in passato dal legislatore, di fronte alla accertata inidoneità dei criteri previsti in via generale dal codice di procedura penale".*

effettuato prima dei due già in atti, in luogo che potrebbe radicare la competenza di una ulteriore e diversa ancora Procura).
Pertanto, anche quale criterio più immediatamente prossimo al principio costituzionale del giudice precostituito per legge, dovrebbero trovare qui applicazione i criteri che vengono valorizzati dal legislatore con la previsione di cui all'art. 9 comma 2 c.p.p.: anche perché, per un dato di comune esperienza difficilmente confutabile, ciascuna persona è solita aprire una carta postepay (e comunque poi riscuoterne le somme) nel luogo più prossimo alla sua residenza, dimora o domicilio.
Tutto ciò posto, l'adesione alla diversa impostazione giuridica indicata dapprima nel 2008 dalla Procura Generale presso la Corte di Cassazione ed oggi dalla Suprema Corte fa riemergere, nelle sue immediate conseguenze concrete, quell' ostacolo all'accertamento dell'esistenza di una serialità nella commissione delle truffe online, dal momento che – in ipotesi – uno stesso indagato potrebbe avere aperto presso ciascuna Procura della Repubblica italiana un solo fascicolo (senza che ciascun Ufficio investigativo possa avere la possibilità di conoscere, in tempo reale, l'esistenza degli altri e quindi procedere in maniera unitaria nei complessivi accertamenti)[37].

5. IL PROTOCOLLO INVESTIGATIVO

Una volta emerse, con le soluzioni organizzative indicate nel par. 3, profili di serialità nella commissione di tale tipologia di reati, la conseguente attività di indagine è scandita dai seguenti punti:

5.1 La iniziale valutazione della competenza territoriale

In tale contesto occorre innanzitutto ben identificare gli strumenti di pagamento (conti correnti e/o carte di credito tradizionali e/o carte di

37 Nelle more di stampa di questo testo la Procura Generale presso la Corte di Cassazione, con decreto n. 224 del 23.9.2015 (est. Romano), *"pur nel doveroso rispetto delle determinazioni della Suprema Corte"* ha confermato il proprio mutamento di indirizzo, ribadendo pertanto che la competenza territoriale vada individuata *"facendo riferimento al luogo di attivazione della carta ricaricata a favore della quale è stato effettuato il versamento da parte del compratore/truffato" ("fino a quando la questione non potrà tornare all'attenzione del giudice di legittimità"*: si noti che, al riguardo, l'estensore cita Cass., Sez. II, n. 7749/2015 la quale ribadisce come *"il delitto di truffa contrattuale si consuma nel luogo ove il reo consegue l'ingiusto profitto e non già nel luogo ove viene data disposizione per il pagamento").* Su tale ultimo punto si sofferma, ancora più espressamente, anche il successivo decreto n. 225 del 23.9.2015 (est. Corasaniti): *"Va infine sottolineato come in linea con l'orientamento di questo Ufficio si pone anche la giurisprudenza maggioritaria della S.C. proprio in relazione a truffe contrattuali via web commesse attraverso un sito di e commerce* (Sez. 2. Sentenza n 7719 del 2015 per cui il delitto di truffa contrattuale si consuma *nel luogo ove il reo consegue l'ingiusto profitto* e non già nel luogo ove viene data la diposizione per il pagamento Cass. 12795/2011; Cass. n. 14950/2009) *ed ancora nello stesso senso Sez. 2 Sentenza n. 43156 del 2013 e Sentenza Sez. 2 n. 4038/2013 concernente poi specificamente anche l'ipotesi di accertamento di ipotesi associativa per il reato di truffa attraverso la ripetuta pubblicazione di fraudolente proposte di vendita su sito internet ai danni di diverse parti offese con articolata organizzazione di ruoli criminosi"*.

credito prepagate ricaricabili) utilizzati dalle parti offese per effettuare i pagamenti dei beni posti fraudolentemente in vendita; ciò al fine di:

a. **accertare il luogo in cui il conto corrente (bancario o postale) risulta attivato dal truffatore** (atteso che, sulla base della consolidata impostazione della Procura Generale presso la Corte di Cassazione negli ultimi anni ed essendosi la Corte di Cassazione occupata solo dalle diversa ipotesi di pagamenti tramite ricariche postepay, in questi casi il luogo di attivazione – inteso come domicilio informatico dell'intestatario – rileverebbe ai fini della individuazione della competenza territoriale);

b. **verificare la residenza dell'intestatario del conto corrente attivato online** (ed infatti, come già ricordato, sempre la Procura Generale presso la Corte di Cassazione ha risolto i contrasti di competenza territoriale accogliendo il criterio residuale *ex* art. 9 comma 2 c.p.p. ritenendo non applicabile il concetto di domicilio informatico dell'intestatario atteso che le cd. banche online sono generalmente prive di proprie filiali e i correntisti possono operare sul conto solamente tramite operazioni telematiche);

c. **individuare il luogo in cui la carta di credito prepagata è stata ricaricata dalla persona offesa/acquirente** (accertamento ugualmente rilevante ai fini della competenza territoriale ove si voglia aderire alla impostazione da ultimo indicata dalla Corte di Cassazione);

d. **verificare il luogo in cui viene concretamente riscosso il vaglia postale** (nei casi di pagamenti eseguiti con questo mezzo).

5.2 La verifica che la persona intestataria dello strumento di pagamento sia effettivamente quella che l'ha attivato e non sia invece vittima di furto di identità

È necessario pertanto:

1. **acquisire la copia di tutta la documentazione** attestante l'attivazione dello strumento di pagamento, ivi compresa la copia dei documenti di identità utilizzati;

2. **verificare l'autenticità dei documenti utilizzati** effettuando appositi accertamenti anagrafici presso gli Uffici servizi demografici dei Comuni (anche attraverso l'acquisizione del cartellino della carta di identità) al fine di verificare la corrispondenza dei dati e soprattutto dell'effige raffigurata nella foto apposta sul documento;

3. **accertare che il documento utilizzato non risulti oggetto di furto o smarrimento** e, in caso positivo, verificare altresì se la denuncia di furto/smarrimento sia veritiera ovvero sia stata presentata dall'intestatario soltanto per cercare di allontanare da sé le responsabilità dei fatti.

5.3 Il controllo che i pagamenti effettuati dalle parti offese attraverso i bonifici o le ricariche siano effettivamente andati a buon fine

Occorre pertanto:

1. **acquisire** dalle banche o da Poste Italiane **l'estratto conto completo** degli strumenti di pagamento utilizzati;
2. **accertare che i soldi** pagati dalle parti offese **siano stati effettivamente accreditati** e la truffa si sia quindi effettivamente consumata.

5.4 La verifica che la persona intestataria dello strumento di pagamento sia anche la reale responsabile delle truffe poste in essere ai danni dei compratori

A tal proposito è necessario:

1. **accertare se l'intestatario dello strumento di pagamento ne abbia anche la reale disponibilità**, essendo a conoscenza anche dei relativi codici segreti/*password* dispositive necessari per il loro utilizzo;

2. **verificare che l'intestatario non sia soltanto un mero prestanome** che viene indotto, con minacce ovvero approfittando della sua situazione di indigenza, ad attivare carte di credito di cui non ha mai il reale possesso e che vengono invece utilizzate da altri per portare a termine le truffe.

5.5 La compiuta identificazione della persona ritenuta responsabile delle truffe

A tal fine pertanto occorre procedere alle *tradizionali* ricerche della persona ritenuta responsabile delle truffe, ricerche sempre molto lunghe e difficili e che spesso non vanno a buon fine dal momento che in genere si tratta di persone senza fissa dimora, cancellate per irreperibilità dagli Uffici Anagrafe dei comuni di residenza, ovvero anche persone straniere (di solito dell'est europeo) che, una volta portate a termine le truffe, preferiscono tornare nei paesi di origine dove monetizzano le truffe attraverso prelievi di danaro dagli sportelli bancomat ivi ubicati.
A margine di tale attività di indagine "tradizionale" (che viene senz'altro privilegiata e che spesso comprende anche analoghi accertamenti sugli intestatari di eventuali utenze telefoniche utilizzate per perpetrare le truffe, accertamenti che ripropongono le medesime problematiche sopra richiamate, in quanto tali utenze risultano nella gran parte dei casi intestate a persone inesistenti o a stranieri irreperibili, o a persone cui è stata rubata l'identità e che quindi ignorano di esserne le intestatarie), in alcuni casi viene posta in essere anche una attività investigativa più specifica e tecnica che mira alla individuazione dei mezzi telematici utilizzati per portare a termine le truffe (con l'acquisizione dei *log files*

relativi alle connessioni internet sia dell'*account* di posta elettronica utilizzato per la pubblicazione online dell'offerta di vendita, sia dell'*account* utilizzato invece per comunicare con il potenziale acquirente durante la fase della contrattazione).
Tali indagini tuttavia, oltre a rivelarsi spesso inutili in quanto riconducono a connessioni effettuate da computer violati o controllati dagli effettivi responsabili all'insaputa dei proprietari (per carenza di protezioni *antivirus*), risentono anche dei limitati termini di conservazione dei dati informatici che i gestori di telecomunicazione sono tenuti a rispettare (in Italia generalmente un solo anno, ma se tali gestori sono stranieri tali termini si riducono anche a pochi mesi), limiti che influiscono in modo sostanziale quando, come nei casi delle truffe seriali, le indagini richiedono molto tempo.
È appena il caso di accennare ad una ulteriore problematica tipica delle indagini su questo tipo di truffe, e cioè l'impossibilità di sapere quando il reato si sia esaurito e il truffatore seriale oggetto di indagine abbia concluso la propria attività criminosa.
In sostanza accade spesso che, una volta concluse le indagini per i procedimenti penali presenti (con la citazione a giudizio del truffatore seriale individuato per tutti i casi in questione), giungano all'Ufficio requirente nuovi fascicoli per altre truffe poste in essere dallo stesso truffatore seriale ma a danno di altre persone offese. In questi casi pertanto, malgrado gli accertamenti sugli strumenti di pagamento siano già stati eseguiti, essi dovranno essere ripetuti con nuove indagini e nuove acquisizioni di documentazione, dal momento che quelli portati a termine in precedenza non possono più essere utilizzati nel nuovo procedimento penale, con una duplicazione delle indagini che allunga ulteriormente i tempi di definizione dei fascicoli presenti in Ufficio.

6. ALCUNI DATI CONCLUSIVI

Il metodo investigativo ed organizzativo che è stato finora descritto ha comportato, quanto all'attività cd. definitoria dei fascicoli pervenuti presso la Procura della Repubblica di Milano in materia di truffe su piattaforme *e–commerce*:

a. trasmissione di fascicoli processuali, riuniti ove siano emersi profili di serialità, alle Procure territorialmente competenti[37];

b. archiviazione[38] dei fascicoli processuali, ugualmente riuniti in caso di medesimo truffatore o *modus operandi*, ove non siano emerse evidenze

37 Nel periodo di riferimento, i fascicoli esauriti con provvedimento di trasmissione ad altra Procura competente sono stati: mod. 21 – 957; mod. 44 – 1.002; totale fascicoli trasmessi per competenza territoriale nel periodo 21 gennaio 2008– 25 maggio 2015: 1959.

38 Nel periodo di riferimento, i fascicoli esauriti con richiesta di archiviazione sono stati: mod. 21 – 781; mod. 44 – 6739; totale fascicoli definiti con richiesta di archiviazione nel periodo 21 gennaio 2008– 25 maggio 2015: 7520.

probatorie o positivi coordinamenti investigativi con altre Procure (come recentemente avvenuto con un procedimento avente oltre 100 persone offese, all'esito di una attività di indagine durata alcuni anni);

c. redazione dell'avviso di conclusioni indagini *ex* art. 415–*bis* c.p.p. per i fascicoli relativi a truffatori seriali ed esercizio unitario dell'azione penale di regola tramite decreto di citazione diretta[39] (attività che risulta difficoltosa non solo per il grande numero di episodi da contestare, ma anche per la redazione della lista testi incorporata al decreto di citazione diretta a giudizio).

Occorre da ultimo ricordare che, in ogni caso, anche gli altri fascicoli vengono analizzati in sede di prima assegnazione indipendentemente dai profili di serialità, soprattutto ai fini di richieste di sequestro preventivo in caso di somme di una certa entità ove ancora presenti su conti correnti/carte ricaricabili.

Dai dati statistici relativi al periodo intercorrente tra il gennaio 2008 e il maggio 2015 è possibile ricavare come i truffatori seriali nei confronti dei quali è stato possibile esercitare l'azione penale sono stati 134[40]: alla luce dei precedenti dati sulla media delle persone offese (e relativi fascicoli) per ogni seriale perseguito, è possibile stimare che tale numero corrisponda a circa 1600/1900 fascicoli trattati.
Proprio avendo in mente l'esperienza dei truffatori seriali, il gruppo di lavoro congiunto che dal 2010 si è costituito (con la partecipazione di esponenti del Comune di Milano e dell'Ordine degli Avvocati di Milano) ha portato ad una prima elaborazione teorica, compendiata nel *working paper "Vittim@ ineffabile"*[41], circa forme di giustizia riparativa. Il tutto come recentemente presentato alla Conferenza internazionale *"Vittime di reato e giustizia penale. Standard europei e buone prassi nazionali"* (Milano, 10 ottobre 2014)[42] e alla *Octopus Conference* del Consiglio d'Europa (Strasburgo, 17 giugno 2015)[43].

39 Non è di fatto utilizzabile lo strumento del decreto penale di condanna, attesa la durata delle indagini di regola non contenibile nei 6 mesi dall'iscrizione.

40 Tale dato sconta tuttavia l'impossibilità statistica di poter tener conto di quanti altri fascicoli attinenti a truffatori seriali siano, alla data del 25 maggio 2015, ancora in attesa di fissazione della data di prima udienza, all'esito trasmissione all'Ufficio pre–dibattimento del relativo decreto di citazione diretta a giudizio: ed infatti il REGE considera "definito" il fascicolo, con esercizio dell'azione penale, solo quando viene fissata la data della prima udienza. Pertanto i fascicoli in attesa di fissazione udienza a seguito di decreto di citazione diretta in giudizio rimangono ancora "pendenti".

41 *Cfr.* nota 3.

42 *Cfr.* nota 12.

43 *Cfr.* il reperibile a partire da *www.procura.milano.giustizia.it/files/Guidelines–to–fight–cybercrimes–and–protect–victims.pdf.*

IISFA è la prima e unica associazione italiana con focus specifico sulla "Information Forensics". L'associazione, senza scopo di lucro e aperta a tecnici e giuristi, ha come mission la promozione della materia, attraverso la divulgazione, l'apprendimento e la certificazione, riconosciuta tra l'altro in ambito internazionale. Le attività ruotano intorno a un codice etico e alla possibilità di far parte di un network di specialisti, con lo scopo altresì di costituire insieme, nel medio periodo, un punto di riferimento nello specifico settore, allo stato sottolineato da forti individualità.
Per altre informazioni: www.iisfa.it

Argomenti: Le truffe su piattorma di *e-commerce*. OSINT. Il monitoraggio dei social network con nodexl. Open source intelligence (OSINT). Windows phone 8 forensics. Frodi interne aziendali e attività investigativa. La prevenzione di comportamenti rischiosi in azienda. Snapchat forensics: il caso. Electronic discovery. Accesso abusivo ad un sistema informatico o telematico. Implementare ipotesi investigative. Nuovi metodi di indagine

Autori: Federica Bertoni, Francesco Cajani, Giuseppe Cattaneo, Fabio Cavallo, Paolo Dal Checco, Silvia Di Iorio, Mattia Epifani, Mattia Falduti, Umberto Ferraro Petrillo, Elisa Fossati, Marilena Guglielmetti, Mario Ianulardo, Demetrio Macheda, Alessandro Massaro, Fabio Mele, Raffaele Olivieri, Fabrizio Perrone, Francesco Picasso, Litiano Piccin, Gianluca Roscigno, Marco Scarito, Giuseppe Specchio, Michela Vecchi

ISBN 9788895694450

Euro 24,00