a cura di GERARDO COSTABILE e ANTONINO ATTANASIO

IISFA Memberbook 2011 DIGITAL FORENSICS

Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER

experta edizioni

CAPITOLO PRIMO

"*DI NECESSITÀ, VIRTÙ*": APPUNTI PER UNA STRATEGIA GLOBALE AL CONTRASTO DEL *CYBERCRIME*. L'ESPERIENZA DEL *POOL* REATI INFORMATICI DELLA PROCURA DI MILANO

Francesco Cajani, Davide D'Agostino, Walter Vannini *

SOMMARIO: 1. L'impatto della legge 48/2008 sulle Procure distrettuali e la necessità di riorganizzare le metodologie di lavoro. - 2. Il problema dei criteri di individuazione della competenza territoriale nelle truffe informatiche attuate con utilizzo di carte ricaricabili (come strumento di pagamento a fronte di un acquisto di beni su piattaforme di e-commerce). - 3. Il sommerso che avanza: i "serial killer" informatici della porta accanto. - 3.1 Casi ed esperienze. - 4. La vittima, al centro. - 5. Per una prima classificazione "esperienziale" delle categorie di reati informatici. - 6. Le Direttive per la Polizia Giudiziaria sui primi accertamenti investigativi in materia di reati informatici e modalità di trasmissione delle relative comunicazioni di notizia di reato alla Procura di Milano. - 7. L'aggiornamento professionale per la Polizia Giudiziaria. – 7.1 Il piano di formazione a distanza (FAD) per il 2012. – 8. Un sito internet informativo per la persona offesa e per la Polizia Giudiziaria. – 9. Una proposta di legge per l'assegnazione alla Polizia Giudiziaria dei beni informatici sequestrati/confiscati nelle indagini informatiche. – 10. In luogo di una conclusione.

1. L'IMPATTO DELLA LEGGE 48/2008 SULLE PROCURE DISTRETTUALI E LA NECESSITÀ DI RIORGANIZZARE LE METODOLOGIE DI LAVORO

È certo diffusa la percezione che l'uso a fini criminali dell'informatica abbia la capacità di procurare danni economici e sociali importanti se messi in rapporto ai mezzi impiegati, non fosse altro che per l'ampiezza della platea a cui il criminale indirizza attenzione e ingegno, ed in cui pesca le proprie vittime. Una attività predatoria capace di incidere velocemente sulla fiducia e sulle aspettative di reciprocità nella relazione sociale ed economica e, per quanto al commercio, un ostacolo formidabile alla disponibilità alla transazione

* Difficilmente un giurista, un investigatore e un criminologo, anche quando per avventura si trovano a parlare delle stesse cose, riescono ad utilizzare il medesimo linguaggio: il lettore quindi ci scuserà se, a volte, le voci del racconto sembreranno assumere accenti diversi… ma anche questo è parte vitale del nostro stare insieme.

ed al consumo.

Fa una certa impressione rimettere oggi mano ai numeri sulla criminalità informatica forniti ogni anno dalla Polizia Postale. Vi sono fenomeni ormai, per fortuna, quasi "debellati": così, quanto alle truffe relative alle numerazioni cd. a valore aggiunto (709, 899, 00[1]), le persone denunciate alla Autorità Giudiziaria[2] dalla (sola) Polizia Postale in Italia sono passate negli anni da 1169 (nel 2003) a 2329 (nel 2004) per poi ritornare a 1821 (nel 2005) e diminuire ancora. Ma, per la maggior parte, gli aumenti di anno in anno sono significativi: siamo soprattutto nel campo degli illeciti relativi al commercio elettronico, con 119 persone denunciate in Italia alla Autorità Giudiziaria dalla (sola) Polizia Postale nel 2004, 203 nel 2004, 566 nel 2005… per arrivare, superate le 4000 nel 2008, a 4582 nel 2009 (con un dato in leggero calo, 3965, nel 2010).

Quanto invece alle denunce raccolte sempre dalla (sola) Polizia Postale in Italia e alle segnalazioni dalla stessa ricevute, anche qui registriamo negli ultimi due anni numeri significativi:

Denunce	**2009**	**2010**
Carte credito	*496*	*481*
E.commerce	*2807*	*2882*
Intrusioni informatiche	*901*	*781*
Phishing	*830*	*762*
Dialer	*205*	*145*

Segnalazioni	**2009**	**2010**
Hacking	*669*	*782*
Pedopornografia	*2227*	*2711*
Altro	*384*	*545*
E.commerce	*367*	*436*
Phishing	*7556*	*6484*

Quasi fosse passato inosservato al Legislatore italiano l'esponenziale aumento (a partire dal 2005) dei reati informatici cd. puri, la legge 48/2008 ha introdotto una ipotesi di competenza funzionale del Pubblico Ministero,

[1] Cfr. *infra* par. 5.

[2] Trattasi di un dato diverso rispetto alle denunce raccolte dalla Polizia Postale, di cui diremo in seguito.

con la previsione di cui all'art. 11 (norma peraltro non strettamente conforme alle previsioni della Convenzione di Budapest, che all'articolo 22 intendeva invece far riferimento ai ben diversi problemi di giurisdizione in materia di *cybercrime*[3]) in vigore dal 5 aprile 2008.

La richiamata norma sancisce che all'articolo 51 del codice di procedura penale è aggiunto, infine, il seguente comma:

> *«3-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente».*

Come da molte parti rilevato[4], la previsione di una competenza distrettuale si è subito mostrata priva di alcuna utilità sostanziale ed anzi ha creato numerosissimi problemi, non solo per il difficile raccordo normativo in relazione all'individuazione dell'Ufficio del Giudice per le indagini preliminari territorialmente competente e per i problemi di diritto intertemporale (rispettivamente risolti dagli artt. 2 e 12-*bis* legge 24 luglio 2008, n. 125)[5] ma anche per ragioni prettamente organizzative: infatti la maggior parte delle neonate "Procure informatiche distrettuali" non avevano, al momento della introduzione della legge 48/2008, magistrati già dediti a lavorare come *pool* nelle materie attinenti la *cybercriminalità* e quindi si sono dovute organizzare

[3] Così F. CAJANI, *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono … Brevi cenni sui problemi di giurisdizione che emergono in tema di intercettazioni telematiche e di* data retention e sui correlativi ostacoli all'azione investigativa di contrasto al crimine*",* in *Ciberspazio e dir.,* 1, 2010, p. 188.

[4] Si consenta ancora il rinvio a 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, pp. 1 e ss. Analoghe preoccupazioni, sia pure rispecchianti il diverso punto di vista della Difesa, in L. LUPARIA, *Computer crimes e procedimento penale,* in *Trattato di procedura penale,* VII, I (a cura di G. GARUTI), Torino, 2011, p. 377: "*il proposito sotteso appare all'evidenza quello di favorire concentrazione e coordinamento, anche se all'orizzonte si stagliano perniciose disfunzioni ed eccessivi ingolfamenti a livello centrale, capaci di incidere negativamente sull'efficienza dell'accertamento e, di conseguenza, sul rispetto dell'obbligatorietà dell'esercizio dell'azione penale".*

[5] In relazione all'ulteriore problema – non ancora specificatamente affrontato dalla giurisprudenza - della connessione fra procedimenti (dei quali solo uno attinenti ai reati informatici oggi distrettualizzati) cfr. F. CASSIBBA, *L'ampliamento delle attribuzioni del Pubblico Ministero Distrettuale*, in AA.VV. (a cura di L. LUPARIA), *Sistema penale e criminalità informatica*, Milano, 2009, pp. 123 e ss.

ex novo.

In tal senso è stata meritevole la sensibilità dimostrata a livello centrale dal Comitato Scientifico del Consiglio Superiore della Magistratura (che ha notevolmente implementato l'offerta formativa per i magistrati sui temi dei reati informatici e delle nuove tecnologie) nonché, a livello decentrato, da alcune iniziative ugualmente meritevoli rivolte anche alla Polizia Giudiziaria[6].

Avevamo già riportato in precedenza[7] il significativo incremento percentuale delle fattispecie di reato informatico trattate presso la Procura di Milano, alla luce della elaborazione statistica relativamente al periodo 5.4.2007/4.4.2008 (data quest'ultima di entrata in vigore della l. 48/2008) e 5.4.2008/4.4.2009, con l'auspicio di un ripensamento del Legislatore, anche considerato che - alle aumentate competenze delle Procure distrettuali, non sono finora parallelamente seguite – come ci si sarebbe ragionevolmente aspettato – azioni legislative volte ad elevare il livello di conoscenza tecnica delle Forze di Polizia Giudiziaria presenti sui rispettivi territori e/o il livello di dotazioni informatiche in uso alle stesse, ancora di gran lunga obsolete – come vedremo nella parte finale di questo scritto - per un adeguato contrasto alla criminalità.

Tale *trend*, a distanza di due anni dall'ultima rilevazione, viene confermato dai seguenti dati[8]:

---

[6] Tra queste merita di essere menzionata quella dell'Ufficio dei Referenti Informatici per il Distretto di Corte d'Appello di Milano - di concerto con il Procuratore della Repubblica presso il Tribunale di Milano ed in collaborazione con IISFA che ha rilasciato gli attestati di partecipazione, validi per ottenere la certificazione CIFI – relativa ad un corso base per gli accertamenti informatici nelle investigazioni penali (il corso - 4 lezioni, per un totale di 14 ore - è stato rivolto nel 2009 sia al personale dell'Aliquota di Polizia Giudiziaria di supporto ai magistrati della Procura di Milano sia - grazie all'adesione della Procura Generale presso la Corte di Appello di Milano - a tutte le Forze dell'Ordine che collaborano con le Autorità Giudiziarie del Distretto di Milano).
Quanto alle realtà universitarie italiane, devono essere qui ricordati – tra gli altri – i corsi di perfezionamento *post laurea* sui temi della *computer forensics* tenuti dall'Università degli Studi di Milano e dalla LUMSA di Roma, nonché il Corso di aggiornamento professionale dell'Università degli Studi di Siena in diritto e tecnica dell'investigazione.

[7] In F. CAJANI, *Considerazioni sull'impatto della "distrettualizzazione" ex legge 48/2008 sul pool reati informatici della Procura di Milano*, op. cit., pp. 3-4.

[8] In assenza di appositi programmi statistici, è solo possibile utilizzare i dati estratti dal registro penale informatizzato: in tal senso, quindi, i numeri sopra riportati fanno riferimento alle singole iscrizioni (e quindi, non necessariamente, coincidono con il numero di fascicoli – dal momento che un singolo fascicolo processuale può essere iscritto anche per diverse ipotesi di reato). Tale estrapolazione, anche se - per la base dati che viene interrogata – può restituire da un anno all'altro la stessa ipotesi di reato laddove il fascicolo venga dal mod. 44/ignoti portato al mod. 21/noti, è comunque significativa per restituire una "fotografia" dei carichi di lavoro, sia per quantità che per qualità (dal momento che un fascicolo a mod. 21 di regola comporta, in ogni caso, una complessità in termini di accertamento maggiore rispetto ad uno a mod. 44).

		5.4.07 4.4.08	5.4.08 4.4.09	5.4.09 4.4.10	5.4.10 4.4.11
615-*ter*	*mod. 21*	53	101	124	220
accesso abusivo a sistema informatico/telematico	*mod. 44*	201	440	586	606
		254	**541**	**710**	**826**
615-*quater*	*21*	13	15	26	24
detenzione/diffusione abusiva di codici di accesso a sistemi info	*44*	22	22	34	35
		35	**37**	**60**	**37**
615-*quinquies*	*21*	1	0	0	0
diffusione programmi diretti a danneggiare sistema informatico	*44*	8	1	5	2
		9	**1**	**5**	**2**
617-*bis*	*21*	4	8	7	3
	44	10	1	5	8
installazione apparecchi atti a intercettare		**14**	**9**	**12**	**11**
617-*ter*	*21*	0	0	1	0
falsificazione/soppressione contenuto comunicazioni telefono	*44*	5	1	5	1
		5	**1**	**6**	**1**
617-*quater*	*21*	4	18	13	12
intercettazione/impedimento illecito comunicazioni info	*44*	5	10	29	15
		9	**28**	**42**	**27**
617-*quinquies*	*21*	0	12	19	17
installazione apparecchiature atte a intercettare	*44*	6	8	26	90
		6	**20**	**45**	**107**
617-*sexies*	*21*	2	2	4	3
falsificazione/soppressione contenuto comunicazioni informatiche	*44*	2	7	3	3
		4	**9**	**7**	**6**

640-*ter*	*21*	57	152	249	348
frode informatica	*44*	1.288	1.602	1.113	767
		1.345	**1.754**	**1.362**	**1.115**
635-*bis*	*21*	3	5	8	14
danneggiamento informatico	*44*	5	8	15	16
		8	**13**	**23**	**30**
635-*ter*	*21*	**	0	0	1
	44	**	0	0	1
			0	**0**	**2**
635-*quater*	*21*	**	0	0	2
	44	**	1	1	2
			1	**1**	**4**
635-*quinquies*	*21*	**	0	0	0
	44	**	0	1	1
			0	**1**	**1**
TOTALE DISTRETTUALI	*21*	**137**	**313**	**451**	**644**
	44	**1.552**	**2.101**	**1.823**	**1.547**
		1.689	**2.414**	**2.274**	**2.169**
TOTALE 640 INFO	*21*	**70**	**344**	**330**	**385**
(da circolare Procuratore 21.1.08)*	*44*	**560**	**1.309**	**1.293**	**920**
		630	**1.653**	**1.623**	**1.305**
TOTALE POOL REATI INFORMATICI	*21*	**207**	**657**	**781**	**1.029**
	44	**2.112**	**3.410**	**3.116**	**2.467**
		2.319	**4.067**	**3.897**	**3.496**

E anche le fattispecie relative alle carte di credito (ipotesi fortunatamente escluse dalla distrettualizzazione *ex* legge 48/2008) sono, ugualmente, in costante crescita:

		5.4.07 4.4.08	**5.4.08 4.4.09**	**5.4.09 4.4.10**	**5.4.10 4.4.11**
carte credito	*21*	***205***	***298***	***388***	***500***
	44	***3.227***	***3.595***	***7.952***	***24.171***

* Nel gennaio 2008 il 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 (coordinatore del *pool* reati informatici) disponeva in tal senso con apposita circolare interna (in vigore dal 21.1.2008).

Rimane infatti tuttora evidente che radicare una competenza distrettuale ricomprendente tutta la gamma dei reati informatici ha significato paralizzare l'azione investigativa, dal momento che anche questioni meramente "bagatellari" (si pensi ad una querela per un accertato malfunzionamento di una casella di posta elettronica) di fatto si aggiungono, come un fiume in piena e senza una ragionevole *ratio*, alle notizie di reato meritevoli di sviluppo[9].

Nel corso degli ultimi due anni tuttavia, pur non mutando il dato numerico con il quale cimentarsi (ed avendo peraltro solo recentemente il *pool* incrementato la sua composizione, passando da 3 a 4 magistrati[10]), siamo stati necessariamente chiamati ad attuare un percorso di riorganizzazione delle metodologie di lavoro, in una prospettiva il più possibile di approccio globale al problema, tenendo in adeguata considerazione tutti gli attori coinvolti al fine di valorizzare le reciproche potenzialità, lavorando insieme sugli aspetti maggiormente problematici.

Di tutto questo, al fine di condividere l'esperienza nella certezza di ricavarne significativi spunti di miglioramento, faremo cenno nel prosieguo di tale contributo.

2. IL PROBLEMA DEI CRITERI DI INDIVIDUAZIONE DELLA COMPETENZA TERRITORIALE NELLE TRUFFE INFORMATICHE ATTUATE CON UTILIZZO DI CARTE RICARICABILI (COME STRUMENTO DI PAGAMENTO A FRONTE DI UN ACQUISTO DI BENI SU PIATTAFORME DI *E-COMMERCE*)

Un primo punto di partenza, in linea con lo spirito della circolare del

[9] Queste le condivisibili valutazioni di Alberto Nobili in una recente nota al Procuratore, in vista della redazione dell'annuale relazione per l'inaugurazione dell'anno giudiziario 2010: "*decisamente rilevante il numero dei cd. Reati informatici (tra i quali, per analogia, possono essere incluse anche le cd. clonazioni di carte di credito) nel cui ambito si sono particolarmente contraddistinti individui di origine rumena dotati di specifiche ed elevate competenze tecniche ed informatiche. Va osservato che presso questa Procura della Repubblica è stata all'uopo recentemente costituita la Sezione di Polizia Giudiziaria Reati Informatici destinata alla disamina, allo studio ed al contrasto dei reati informatici seriali con il conseguimento, proprio di recente, di lusinghieri risultati. Parlando di Reati Informatici non può tacersi il grave ed ingiustificato aggravio di lavoro per questa Procura della Repubblica determinato dalla introduzione dell'art. 51 quinquies del codice di procedura penale (v. "distrettualizzazione dei reati informatici") a seguito del quale una qualsiasi intrusione informatica (ad esempio quella di una marito geloso di Sondrio che "sbircia" nel computer della moglie), una qualsiasi frode informatica commessa a Pavia, Varese, Como, Lodi etc., una qualsiasi captazione di dati da un qualsiasi apparecchio Bancomat di Busto Arsizio, Vigevano o Monza dovrà essere trattata, investigativamente parlando e senza alcuna seria plausibile ragione, da questa Procura della Repubblica di Milano. Il disegno normativo avrebbe forse potuto avere una sua ragion d'essere solo ove finalizzato a migliorare le attività di contrasto nei confronti di fenomeni di criminalità informatica riconducibili alle attività di gruppi organizzati strutturati in ambito associativo".*

[10] Massimiliano Carducci, Elio Ramondini, Adriano Scudieri (oltre a Francesco Cajani). Fino alla metà del 2010 ha fatto parte del *pool* reati informatici anche Elisa Moretti e, prima ancora, Gianluca Braghò

gennaio 2008[11], era stato quello di affinare la capacità interna di incrociare dati provenienti da molteplici querele ma in un settore specifico (e non omnicomprensivo come poi avvenuto con la legge 48/2008), quale quello delle truffe cd. *eBay* (o relative ad altre piattaforme *di e-commerce*), ultima frontiera dei reati informatici (ugualmente in aumento nella loro molteplicità di forme di manifestazione, come abbiamo visto).

La stessa creazione, nel maggio 2007 all'interno della Procura di Milano, di una "Squadra di PG reati informatici"[12], era stata anche finalizzata a dare un risposta più efficace in tale direzione: perché anche in tale settore possiamo parlare di "*serial killer*", dotati di armi sia pur non mortali quali i personal computer ma ugualmente lesive.

A complicare ancor di più qualsiasi tentativo di raccordare l'azione investigativa a livello nazionale vi è la incertezza, nella richiamata materia, dei criteri di determinazione dei criteri di competenza territoriale.

Fino al 2008, il criterio tradizionalmente seguito da molti Uffici Giudiziari requirenti era quello del luogo di conseguimento dell'illecito profitto, identificato nel luogo di apertura del conto corrente beneficiario 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 mai dimenticato: infatti, in relazione a tale tipologia di reato (ove il discrimine con una mera 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 sarebbe stato 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.

Una simile "concentrazione" può 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

[11] Come già ricordato, la circolare del Procuratore della Repubblica presso il Tribunale di Milano Manlio Minale del gennaio 2008 disponeva la concentrazione anche dei fascicoli attinenti le truffe su piattaforme informatiche *ex* art. 640 c.p. in capo al *pool* reati informatici.

[12] Attualmente tale Squadra è composta da 8 persone, provenienti da tutte le forze di polizia presenti sul territorio – Polizia di Stato, Carabinieri, Guardia di Finanza, Polizia locale: essa è di supporto al *pool* reati informatici ma anche ad accertamenti informatici in indagini in carico ad altri magistrati della Procura, ove riservatezza o complessità degli stessi lo rendano opportuno. Sul punto cfr. M. CARDUCCI, *Il pool reati informatici nella Procura di Milano: i rapporti con la Polizia Giudiziaria e la Magistratura estera*, in *Atti del Convegno OLAF "Nuove prospettive dell'attività investigativa nella lotta antifrode in Europa" - Milano, 24/25 gennaio 2008*, Bruxelles, 2008.

Generale presso la Corte di Cassazione con provvedimento del 24.1.2008[13], in sede di risoluzione dei contrasti negativi di competenza *ex* art. 54 c.p.p. proprio in relazione alle cd. truffe informatiche poste in essere con l'utilizzo di carte ricaricabili, così massimato[14]:

> "*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, giacché l'arricchimento è costituito dalla mera disponibilità, non già dell'effettiva spesa o prelievo della somma*".

Tale impostazione giuridica finisce così di fatto, nelle sue immediate conseguenze concrete, per costituire un ulteriore 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).

Occorre tuttavia segnalare come di recente lo stesso Procuratore Generale – su sollecitazione della Procura di Milano - sia intervenuto 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[15], valorizzando qui –

---

[13] Nr. 20/2A/2008 PG – 28/08 R.D. Così la motivazione: "*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 Maggio Udinese; [..] contestualmente, con la disponibilità cioè sulla carta di cui è in possesso, della somma versata si verifica l'ingiusto profitto dell'agente, a 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"*.

[14] 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.

[15] In questi casi di regola è immediatamente possibile risalire alla banca interessata laddove sia

quale momento consumativo – "*l'effettivo conseguimento dell'ingiusto profitto da parte degli agenti, con la conseguente concreta e definitiva perdita del bene subita dalla parte offesa, ...avvenuto soltanto ... con l'accreditamento della somma e il positivo esito del disposto bonifico bancario sul c/c predetto*" [16].

---

indicato dalla persona offesa il codice IBAN di tale istituto beneficiario.
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.

[16] Provvedimento del 29.10.2009 n. 241/2A/ 2009 Reg. P.G. - 254/09 R.D. (est. Passacantando). Se ne riporta per completezza la motivazione:
"*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 sì 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, Migliorini, in C.E.D., rv.: 226745; Cass. Sez. II, ud. 28.10.1997, n. 1136, dep. 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/o Poste Italiane in Modena intestato ai due sopra menzionati indagati, e, quindi, l'effettivo conseguimento dell'ingiusto profitto da parte degli agenti, con la

In tali ipotesi quindi si ritorna ad applicare i criteri tradizionalmente seguiti da molte Procure già prima del 2008 (e, a dire il vero, anche in ipotesi di pagamenti della persona offesa a mezzo di ricariche *postepay*), criteri che meglio riescono a soddisfare quelle esigenze di "concentrazione" di episodi delittuosi relativi allo stesso autore in capo ad un unico organo investigativo (prima che giudicante).

Ove poi tali pagamenti, a mezzo di bonifico della persona offesa, vengano effettuati a favore delle cd. banche *online*[17], occorrerà ricorrere ai criteri di cui al secondo comma dell'art. 9 c.p.p. (salvo verificare, tramite analisi del conto corrente, il luogo nel quale l'indagato abbia di fatto posto all'incasso la somma a lui illecitamente trasmessa con bonifico) non essendo possibile identificare *sic et simpliciter* in Milano (ove la maggior parte delle richiamate banche hanno la sede legale) il luogo di conseguimento dell'illecito profitto.

3. IL SOMMERSO CHE AVANZA: I "*SERIAL KILLER*" INFORMATICI DELLA PORTA ACCANTO[18]

Tra le molte attività criminali a mezzo computer, la truffa *online* genericamente intesa è presumibilmente, a livello nazionale, il reato con tassi di crescita relativa più elevati. Si tratta a ben vedere di attività illecite spesso non produttive di grandi danni materiali per la singola vittima, per il singolo evento, ma rilevanti per l'insieme delle somme cumulate e pericolose perché suggestive 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*

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)".

[17] Trattasi di Fineco Bank, Banca Mediolanum, WeBank, IWBank o INGDirect, ossia di istituti di credito pressochè privi di sportelli sul territorio (ed infatti, proprio per tali motivi, si parla di banche *online*).

[18] Per mandato istituzionale, per l'interesse a tutelare vittime e mercati, il *pool* reati informatici della Procura della Repubblica presso il Tribunale di Milano ed il Comune di Milano hanno avviato una collaborazione in tema di lotta al crimine informatico. Le osservazioni che seguono sono debitrici anche di questa collaborazione. Il paragrafo è povero di note e rinvii: si tratta infatti di una prima riflessione e comunicazione di 'lavori in corso', in presa diretta sulla esperienza investigativa in alcuni casi ancora in essere. Definite alcune opportunità allo stato virtuali, una successiva elaborazione conterrà i dovuti rinvii alla letteratura ed all'esperienza.

componente per più versi seduttiva, della distanza (di luogo e di tempo) dal fatto, e dalla virtuale (ahimè concreta) vittima"[19].

Convincere un adulto a consegnare una parte del proprio risparmio ad uno sconosciuto che si presenta e con una scusa lo chiede, è una cosa. Altra cosa è convincerlo a consegnare *tutto* il proprio risparmio al medesimo sconosciuto, che neppure si presenta, che si limita ad inviare un modulo da compilare per improbabili verifiche della *password* o vendere un qualche cosa, con uno sconto che già quello è un affare incredibile in sé.

La prima rappresentazione è improbabile nell'esito, la seconda più che possibile.

Per quanto bizzarra, approssimativa o sgrammaticata sia la richiesta, le denunce restituiscono il numero vasto di persone adulte che hanno compilato il modulo. Adulti che mai avrebbero consegnato i propri codici ad un uomo in carne ed ossa, per quanto travisato da serio funzionario di banca, consegnano le proprie chiavi di casa ad un modulo, una cosa, che compare sul monitor.

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 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.

Fatta salva ogni riflessione sulla qualità della minaccia, l'esperienza investigativa recente sulle truffe via informatica restituisce una casistica che conferma la premessa: tanto il bacino delle vittime è vasto ed indifferenziato, tanto la casistica della persona che agisce la truffa è differenziata; casistica

[19] E. PANZETTI, "*Note sulla psicologia della vittima e dell'incorporeità*", *paper* non pubblicato, Comune di Milano, ottobre 2011.

popolata da identità così lontane tra loro da suggerire l'ipotesi di lavoro per cui ognuno di costoro, agendo la truffa, costituisce la propria nicchia ecologica, l'ambiente virtuale e congruo in cui operare, e - così facendo - toglie la persona, la vittima potenziale, dall'indifferenziato e dal virtuale e la costituisce come vittima specifica e reale. Comprendere la nicchia ecologica è nel contempo un luogo, un contesto significativo, per l'osservazione della vittima, della sua identità sociale ed è - nel medesimo tempo - il luogo attraverso cui individuare la logica intrinseca che governa l'azione criminale, i caratteri specifici, soppesarne la pericolosità, tentare una previsione sull'evoluzione criminale, depotenziarne la virulenza attraverso la sensibilizzazione mirata alle vittime potenziali. In particolare, quest'ultima azione è esattamente qual che accade in internet ogni volta che un evento si ripete e diviene fenomeno identitario per molti. E' ciò che porta alla nascita del forum, della lista, dell'aggregazione tematica virtuale. Meccanismo che gode di virtù analoghe e contrarie all'utilizzo malevolo dei computer. Un fatto che presenta più aspetti di interesse per chi abbia l'obiettivo di contrastare illiceità e abuso.

3.1 Casi e esperienze

Ad una tacca delle truffe via computer - difficile dire se sia un estremo delle possibilità date - possiamo collocare il truffatore segnato dallo stigma sociale dell'inadeguatezza, della povertà in senso qualitativo, dalla personalità fragile, mossa nell'agire illecito da un bisogno intimo, con finalità auto-referenziali, soggetto orientato all'azione individuale, alla messa in scena di una identità tanto artefatta quanto adeguata ed intrigante, da offrire sul palcoscenico virtuale della relazione uno a molti.

Caso reso famoso da servizi televisivi, per dire quanto ignoto volesse rimanere, di un truffatore che si inventa – lui, che nella vita di tutti i giorni è schivo, corpo dimesso e trascurato - una trasmissione via web di telecronaca delle partite in corso, in cui, millantando l'altrui identità, sfoggia presenza e competenza ed un intercalare professionale di commentatore sportivo navigato. E intanto la scritta scorrevole sullo schermo invita a versamenti solidali - sul suo conto corrente, ovvio - per i terremotati. È il medesimo che commercia sulle piattaforme elettroniche, e compresa l'opportunità della vendita fittizia, intuisce il punto debole delle procedure di trasferimento postale del denaro, e così imperversa sulle vittime.

Diventa un motivo di aggregazione sociale delle stesse, ma non solo: *blog* vengono costruiti per socializzare la truffa subita, messaggi di avviso ai naviganti vengono inviati nei *forum* a prevenire l'inganno. Identificato il truffatore con

nome e cognome ci si scambia l' informazione in Rete. *Ovviamente*, lui non fugge. Ma partecipa, spiega, dibatte, si appella, dichiara la difficoltà contingente che gli impedisce di essere puntuale nelle consegne. Più che il non poco denaro acquisito con truffe seriali e subito speso, sembra importagli di essere interlocutore, anzi oggetto di discorso. A questo non si sottrae[20].

Ad un'altra tacca - più affollata, forse - troviamo personalità dotate di buone risorse, individui bene o ottimamente acculturati, esito di percorsi formativi idonei ad una socializzazione conforme, talvolta universitari in corso di studi o giovani imprenditori, capaci di muoversi in modo congruo in ambiti sociali e culturali estremamente differenziati, transnazionali se del caso, in funzione delle necessità di progetto o di studio della truffa: fruizione di reti e servizi criminali esterni e funzionali all'impresa, reperimento delle competenze tecniche, attuazione di un'organizzazione che si estende in più Stati, apprezzamento sociologico dei comportamenti quotidiani del campo delle vittime, delle regole vigenti nel paese terzo e delle opportunità tecniche disponibili, capacità relazionale di molti a molti.

Molestatori di conti correnti, violati a base di *phishing*, acquirenti di documenti falsi per ottenere codici fiscali veri, utili alla sottoscrizione di carte

[20] Cfr. la sentenza di condanna in primo grado alla pena finale di anni cinque, mesi sei e giorni 20 di reclusione ed euro 3200 di multa, oltre al pagamento delle spese processuali (Tribunale di Milano, sentenza 30 aprile 2010 - est. Tutinelli), confermata da Corte d'Appello di Milano, sez. IV, 6 maggio 2011, n. 1310 (est. Crivelli): "*Per quanto concerne la qualificazione giuridica dei fatti, di cui non è contestata la commissione da parte del M., va riaffermato il concorso tra i reati di truffa (art. 640 c. pen.) e di quello previsto dall'art. 55 c.9 d.lgs. 21 nov.2007 n.231, essendo il primo reato integrato dagli artifici e raggiri consistenti nell' aver posto fittiziamente in vendita, sotto falso nominativo, su siti internet, beni (telefoni cellulari ed altro) di cui l'imputato non aveva la disponibilità, inducendo la vittima ad un atto di disposizione patrimoniale consistente nel versamento del prezzo presso un ufficio postale, e concretandosi il secondo reato di utilizzo senza titolo di strumento di pagamento (art.55 c.9 d.lgs.23112007), nell' aver ottenuto,- tramite indici elaborati dal M. o carpiti alla vittima che intendeva, viceversa, fornire il codice segreto per il prelievo della somma depositata solo dopo il ricevimento della merce promessa-, il pagamento da parte dell'ufficio postale di vaglia postali rapidi che dovevano esser incassati solamente da chi conoscesse il codice di accesso fornito dall'Ufficio postale, con una procedura che, come si è riscontrato ex post, non tutelava, invece, adeguatamente la segretezza dell'accesso all'operazione.*

Non risulta in alcun modo che le vittime del raggiro, che intendevano, infatti, garantirsi con il preventivo ricevimento della merce, mai inviata, abbiano volontariamente portato a conoscenza del M. la parte del codice alfanumerico necessaria per incassare le somme disponibili nell'ufficio postale.

Il danno patrimoniale per le vittime, ed il corrispondente arricchimento del M. costituente il delitto di truffa, comportava, perciò, per la sua realizzazione, la violazione di un'ulteriore norma penale, autonomamente prevista dall'art.55 c.9 d.lgs.2312/91 ed intesa ad impedire l'indebito prelievo di denaro contante, realizzato nella specie mediante l'illecita intromissione nel sistema di pagamento dei vaglia postali rapidi […]".

prepagate pensate per il gioco legale e qui prontamente impiegate per riciclare denari altrimenti gravati da costosi oneri di trasferimento.

Menti agili e non banali, come si vede.

Nello spazio della casistica riscontrata, si tratta di operatori di giovane o giovanissima età (secondo i nostri standard), adesivi a modelli di economia dissipativa, con scarsa o marginale propensione alla accumulazione, alla diversificazione di impresa ed al re-investimento degli utili; con una preferenza per la selezione dei compartecipi, di criteri affettivi o di prossimità, etnica, parentale o amicale, senza particolare attenzione alle competenze o all'affidabilità.

In questo senso organizzazioni giovani, a bassa pericolosità in quanto organizzazioni, in cui la prospettiva dello sviluppo dell'impresa è subordinata al benessere qui ed ora dei partecipi talché gli aspetti organizzativi realizzati non tengono in conto delle molte perdite economiche derivate da comportamenti non attesi, attuati da devianti entro la stessa organizzazione, l'assenza di strutture specializzate di controllo interno, di investimenti per la crescita, e così via[21].

Anche qui, più che nel caso precedente, è un insorgere di vittime che si organizzano, che danno vita a *forum* sul *phishing*, ma anche di comportamenti inattesi, come coloro che, avendo ingenuamente dato i codici di accesso al proprio conto, ad indagine avviata, appreso dell'esistenza individuazione della banda e del reato, mantiene invariati il conto, i codici, la *password*. E la possibilità di un nuovo accesso abusivo.

4. LA VITTIMA, AL CENTRO

Ecco, appunto, la vittima. Persona non ignorata dalla criminologia, dalla psicologia, dalla sociologia e dalla storia. Soggetto della vittimologia, dell'antropologia e della filosofia. In tempi relativamente recenti portata concretamente al centro dell'agenda pubblica dalle teoriche della mediazione e delle prassi riparative, così come - in altro verso - dai movimenti civici di solidarietà attiva nati per reazione ai fenomeni della criminalità organizzata più feroce, pur tuttavia la vittima resta fuori dal momento emotivamente intenso e prezioso dell'incontro con l'Istituzione che raccoglie la denuncia.

È il momento in cui, il reato subito, da esperienza privata diviene fatto

[21] Cfr. la recente sentenza di condanna in primo grado, a seguito di giudizio abbreviato, del Tribunale di Milano, 21 febbraio 2011 - est. Manzi, Giudice per l'udienza preliminare. Sul tema si consenta il rinvio a M. GATTI, W. VANNINI, *Persone semplici, organizzazioni complesse: un caso di phishing transazionale. L'operazione Oracolo, problematiche e suggestioni,* intervento a IISFA FORUM 2011 - Milano, 13 maggio 2011.

istituzionale, e perciò pubblico, con lo stigma che ne può conseguire: si pensi alle vicende della diffamazione, al partner che divulga aspetti intimi della persona oppure - e per quanto alle imprese - alle attività di violazione del segreto professionale e di impresa, alla violazione dei sistemi di sicurezza e tutela dei dati sensibili, alle attività minatorie a fini estorsivi e altro ancora. Comprensibile la poco invidiabile condizione dell'impresa i cui sistemi di sicurezza sono stati violati, del professionista cui sono state sottratte informazioni, della persona che vede diffusa la propria intimità ed il rischio che questo divenga stigma, segno caratterizzante. A danno si aggiunge la preoccupazione di un ulteriore danno.

Nel nostro ordinamento processual-penale la vittima è un attore ancillare, non determinante la legittimità del processo. Parte civile, al più con funzioni di stimolo ad una astratta efficacia del processo penale, sempre che il costo di esserci valga la pena. Eppure la vittima è l'istanza da cui prende le mosse l'indagine: prova che un *vulnus* al legame sociale è stato inferto; fonte usuale di *notitia criminis*; ordinaria precondizione della azione penale. Ecco che la vittima è presto resa muta dalla distanza, dai tempi dell'attività requirente e poi da quelli del processo e dei gradi di giudizio. Attore irrisolto, marginalmente utilizzato, salvo per le necessarie informazioni preliminari, gli resta l'eventuale umana sensibilità di un operatore della giustizia, di Polizia o PM, che lo renda in qualche modo partecipe - ma con un lavoro fuori orario, diciamo così.

Una sottovalutazione che i mezzi di informazione amplificano, perché eleggono a mostro il carnefice, perché il processo scagiona l'imputato. Mentre la vittima resta sullo sfondo, riferimento remoto della scena pubblica.

Al contrario, calco della potenzialità dell'informatica usata per operare il raggiro, nei *forum*, nelle *mailing list*, nei *social network*, la vittima dà voce alla propria frustrazione di attore dimenticato: gabbato prima, inoperoso poi, soggetto pubblico eppure solo. Informali gruppi di *self-help* costituiscono opinione pubblica organizzata, critica istituzionale e solidarietà civica. Reti di pari restituiscono indicazioni utili, formazione, riconoscimento e solidarietà. Partecipando, rispecchiandosi in altre vittime, la vittima diventa meno sola, meno inadeguata, socialmente riconosciuta.

Vale la pena spendere una riflessione su questa capacità della rete di essere luogo di vaccini e contro-reazioni efficaci. A Milano ci stiamo provando, pensiero in divenire.

Questo aspetto, il vuoto pneumatico che intercorre tra l'essere stato costituito come vittima e la formalizzazione di un processo di là da venire, è un tempo che potrebbe rivelarsi prezioso per le istituzioni e per la vittima. Anche con atti semplici, anche con atti indiretti. Le "Direttive milanesi", discusse nei prossimi paragrafi, in tal senso già lavorano. Invitano gli Ufficiali di PG, all'atto del primo contatto, ad illustrare alla vittima con miglior dettaglio

alcuni aspetti procedurali, ne promuovono un ruolo più attivo, per esempio nel reperimento dei primi elementi suscettibili di divenire prova o delle tracce da cui muovere l'indagine. Allo stesso modo altre idee sono allo studio: atti di riconoscimento e riparazione verso le vittime; coinvolgimento di Enti pubblici per una più mirata prevenzione, partners di processi formativi indirizzati al personale di Polizia Giudiziaria ed al pubblico; giacimenti di informazione di pronto impiego formativo rivolte a figure adulte con ruoli educativi, a tutela da un uso aggressivo, malevolo, di Internet[22]; la riflessione se non possa essere pensato un impegno diretto degli organi ispettivi nei *forum* che spontaneamente si creano attorno ad un truffato (bizzarro pensare ad un "*agente del thread*" palese? Sorta di evoluzione telematica del poliziotto di quartiere, figura poi non così lontana dagli impegni istituzionali che hanno la forma dei siti istituzionali informativi); incontri nelle scuole e riflessione progettuale sugli investimenti notevoli che le Istituzioni, tutte, fanno per svolgere una azione - peraltro dovuta - di informazione rivolta al pubblico… e, ancora, perché non pensare ad un coinvolgimento del terzo settore e delle associazioni che a vario titolo si occupano delle vittime, non escluse le associazioni di tutela dei consumatori?

5. PER UNA PRIMA CLASSIFICAZIONE "ESPERIENZIALE" DELLE CATEGORIE DI REATI INFORMATICI

Con queste considerazioni sulla figura della vittima e di un ruolo meglio adeguato delle Istituzioni, con queste ipotesi di lavoro in mente, sia pure con tutte le difficoltà sopra indicate, la riorganizzazione dei metodi di lavoro a seguito dell'avvento della legge 48/2008 ha indotto riflessioni e sperimentazioni operative, talvolta preliminari, talvolta parallele - in un gioco di suggerimenti reciproci – a quelle dell'incrocio dei dati per identificare le serialità non palesi, lo studio delle forme e contenuti dei processi criminali specifici e l' integrazione con una riflessione socio-criminologica dei protagonisti, anche involontari, del crimine informatico.

Orbene, uno degli aspetti procedurali che più ha indotto una riorganizzazione delle metodologie riguarda la fase iniziale, immediatamente successiva all'acquisizione della *notitia criminis* ad opera della Polizia Giudiziaria. Il riferimento puntuale su cui vogliamo attirare l'attenzione è il termine temporale entro cui avviene la trasmissione della comunicazione di notizia di reato (cd. CNR).

Ai sensi dell'art. 347 c.p.p. "*acquisita la notizia di reato, la polizia giudiziaria senza ritardo riferisce al pubblico ministero, per iscritto, gli elementi essenziali del fatto e gli altri elementi sino ad allora raccolti, indicando le fonti di prova e*

[22] Per un primo esperimento sul punto si consenta il rinvio al sito *www.virtualeconcreto.net.*

le attività compiute, delle quali trasmette la relativa documentazione".

L'indicazione temporale ("*senza ritardo*"), introdotta dalla novella del 1992 al posto delle originarie "*quarantotto ore*" e che lascia oggi alla Polizia Giudiziaria un margine di autonomia operativa, merita un duplice approfondimento proprio alla luce dell'oggetto del nostro discorso.

Ed infatti, dati i ristretti termini di conservazione dei dati (cd. *data retention)* oggi in vigore, è quanto mai opportuna una celere trasmissione della CNR al fine di ottenere l'idoneo provvedimento di acquisizione, presso i gestori di comunicazione, dei dati relativo al traffico telematico ad opera del Pubblico Ministero.

Si tratta, in ogni caso, di trovare un giusto contemperamento tra esigenze contrapposte: infatti, se da un lato il problema sopra indicato è di effettiva portata pratica, dall'altro è frequente che alla acquisizione della mera *notitia criminis* possano (anzi, debbano) seguire alcuni accertamenti volti ad acquisire i primi riscontri investigativi per autonoma iniziativa della Polizia Giudiziaria.

E dunque un ritardo nella trasmissione della comunicazione di notizia di reato sarà da considerarsi ingiustificato – ed in tal senso passibile di sanzioni[23] - solamente ove lo stesso sia stato, in quanto eccessivo, tale da pregiudicare la persecuzione del reato.

Tutto ciò premesso e stante l'esponenziale aumento del flusso di fascicoli pervenuti nella materia del *cybercrime*, per prima cosa si è ritenuto opportuno – in un'ottica di riorganizzazione del lavoro – elaborare una classificazione della tipologia di casi ogni giorno affrontati, di competenza tabellare[24] del *pool* reati informatici della Procura di Milano anche se non rientranti nelle previsioni della legge 48/2008[25].

Come meglio diremo, una pronta individuazione della categoria di appartenenza è utile per meglio porre in essere – ad opera della Polizia Giudiziaria - gli accertamenti minimi di volta in volta richiesti.

Ancora prima, una pronta individuazione della categoria di appartenenza è utile agli Uffici di Procura dal momento che – a fronte di una aumento di comunicazioni di notizie di reato in materia informatica – è fondamentale una

[23] Sanzioni disciplinari (art. 16 disposizioni di attuazione c.p.p.) e penali (art. 361- 363 c.p.)

[24] Ad eccezione delle carte di credito e delle diffamazione online, non di competenza tabellare ma spesso inerenti a fascicoli comunque trattati dal *pool.*

[25] Furto identità semplice, truffa *eBay* o su altra piattaforma, riciclaggio elettronico dei proventi illeciti (*cyberlaundering*), carte di credito **(s**alve le ipotesi ex art. 617-*quinquies* c.p. - installazione di apparecchiature atte ad intercettare la comunicazione intercorrente tra il chip della carta di credito e il sistema informatico dell'istituto di credito – o ex art. 615-*quater* c.p. laddove con tale condotta - di regola accompagnata anche dalla acquisizione, tramite meccanismi di videoripresa, dei relativi codici PIN all'atto della loro digitazione - abusivamente l'agente si procura codici di accesso al sistema informatico della banca), diffamazione *online*.

organizzazione del lavoro a partire da schemi standardizzati condivisi con la Polizia Giudiziaria.

Anche per questi motivi, il *pool* reati informatici beneficia, dal 2009, della consulenza di un sociologo e criminologo clinico distaccato dal Comune di Milano[26].

A miglior chiarimento, esito di un lavoro che ha visto più professionalità coinvolte in numerose sessioni, fin dal *brain-storming* iniziale, è forse utile mostrare una esemplificazione degli *standard* procedurali elaborati, con la qualificazione giuridica di ogni fattispecie proposta dal *pool* milanese ed una breve descrizione operativa del fatto concreto*:*

- DIALER (NUMERAZIONI A VALORI AGGIUNTO)

QUALIFICAZIONE GIURIDICA: *art. 640-ter c.p.*

FENOMENO:

A) L'utente, navigando in Internet da una rete fissa, scarica senza rendersene conto, ovvero non leggendo con attenzione le schermate di avviso sul dirottamento della chiamata verso numerazioni con un costo maggiore, taluni ***programmi autoinstallanti denominati "dialer"***[27] *che disconnettono il modem e lo ricollegano a numeri a valore aggiunto 899*[28] *e a codici satellitari ed internazionali (00), comportando dei costi molto elevati per la chiamata.*

B) A tale tipologia deve essere equiparato il fenomeno delle ***indebite tariffazioni per traffico dati (Internet)*** *in relazione a schede telefoniche cellulari, connessioni che vengono disconosciute in quanto ugualmente risultanti da bolletta telefonica.*

- FURTO DI IDENTITÀ SEMPLICE

QUALIFICAZIONE GIURIDICA: *artt. 494 c.p.* [29]

[26] Sul punto cfr. anche il rendiconto annuale delle attività della Procura di Milano (1 luglio 2010/30 giugno 2011) a firma del Procuratore Edmondo Bruti Liberati, pp. 52-53, in *http://media2.corriere.it/corriere/content/2011/pdf/relazione_25_luglio.pdf.*

[27] I dialer sono abbinati a volte a siti che propongono di scaricare contenuti, come loghi, suonerie, sfondi, file mp3, immagini e foto pornografiche, oppure sono camuffati da certificati di protezione di Internet Explorer, o sono programmi "activex", che si installano sul pc senza la necessità di scaricare alcun elemento.

[28] I codici 899 sono assegnati dal Ministero delle Comunicazioni alle società o ai gestori telefonici che ne fanno richiesta. Sono previsti una dichiarazione sostitutiva di notorietà sul tipo di servizio offerto tramite il prefisso 899 da effettuare preventivamente prima dell'avvio del servizio ed un messaggio sull'indicazione del costo della chiamata e sul tipo di servizio offerto.

[29] Cass, Sez. 5, Sentenza n. 46674 *del* 08/11/2007 Ud. (dep. 14/12/2007) in CED 238504: "*Inte-*

***FENOMENO**: trattasi di un fenomeno variegato, ricomprendente:*

A) tutti i tentativi di phishing[30] tramite invio di e-mail (in questo caso la più corretta qualificazione giuridica deve essere quella di 56, 494, 640-ter c.p.)

B) altri furti di identità, anche consumati, rispetto ai quali la persona offesa non lamenta di aver ricevuto – al momento della denuncia/querela – un danno.

- VIOLAZIONE ACCOUNT

***QUALIFICAZIONE GIURIDICA**: artt. 494 c.p., 615-ter c.p.*

---

gra il reato di sostituzione di persona (art. 494 cod. pen.), la condotta di colui che crei ed utilizzi un "account" di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete 'internet' nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, subdolamente incluso in una corrispondenza idonea a lederne l'immagine e la dignità (nella specie a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale)"

[30] Il termine "*phishing*" indica un'attività fraudolenta in genere perfezionata sulla rete Internet, che consiste nella predisposizione di tecniche idonee a carpire fraudolentemente dati personali sensibili (quelli più di interesse sono le numerazione di carte di credito, i conti correnti *online*, i codici relativi a depositi effettuati in banca ed i pin dei bancomat, ovvero informazioni che per essere ottenute richiedono anche l'involontaria ma incauta collaborazione della vittima).
L'autore dell'attacco di *phishing* si limita ad inviare ad un numero elevato di utenti della Rete un elemento di stimolo, che in genere consiste in un messaggio di posta elettronica o di un virus informatico, sperando nel ritorno di dati sensibili (*user-id* e *password*) da parte delle vittime, così da accedere a loro conto corrente bancario o postale.
Con l'invio del messaggio di posta elettronica, l'intenzione dei truffatori è quella di far visualizzare il sito relativo al link inserito nell'*e-mail*, ovvero una pagina web clone dell'istituto di credito gestita dai criminali, ove l'utente viene invogliato ad inserire le proprie credenziali di accesso, così acquisite per gli usi illeciti.
Cliccando sul link proposto, infatti, **la pagina che viene caricata non è quella della banca,** dell'istituto o della società corretta, **ma quella di un sito web creato ad arte per consentire all'utente malintenzionato di sottrarre e memorizzare le informazioni fornite da utenti ignari**: informazioni riservate e confidenziali come il nome utente e la password.
Più difficile da percepire risulta l'attacco informatico allorché lo stesso si realizzi attraverso l'invio di un virus - a volte contenuto all'interno della posta elettronica, a volte trasmesso attraverso prassi di navigazione o di sollecitazione di altri servizi Internet se il PC non è dotato di idonea protezione -, che una volta subdolamente installatosi nel personal computer della vittima ne possa carpire i dati sensibili per trasmetterli riservatamente in un secondo momento al truffatore.
Una volta che i criminali abbiano avuto accesso, con le modalità prima descritte, ai dati delle vittime, sono pronti per la sottrazione illecita del denaro contenuto nei loro conti e di far perdere le loro tracce mediante trasferimenti bancari, avvalendosi della complicità di più o meno consapevoli intermediari.

FENOMENO:

Trattasi di un fenomeno più complesso rispetto al precedente, ricomprendente in particolare:

A) ***violazione account eBay o di altre piattaforme di commercio elettronico (o di bacheche annunci vendita)****, al fine di porre fittiziamente in vendita su Internet – avvalendosi di una identità non corrispondente al reale venditore - beni con l'intento di non inviarli all'acquirente, così ottenendo l'ingiusto profitto del prezzo che di regola viene corrisposto tramite pagamenti elettronici prima dell'invio del bene. Di tale fenomeno spesso l'utente (che ha subito la violazione del proprio account) ne viene a conoscenza a seguito della comunicazione che lo stesso si vede recapitare dall'Istituto di recupero crediti Intrum Justitia*[31] *o altri istituti di recupero crediti di transazioni online*[32]

B) ***violazione/acquisizione indebita dell' account personale/profilo Facebook o di quello relativo ad altre piattaforme di social network***

- ACCESSO EMAIL

QUALIFICAZIONE GIURIDICA*: art. 615-ter c.p.*

FENOMENO:

A) trattasi di una ipotesi specifica rispetto a quella precedente che, per la sua diffusività, merita di essere trattata separatamente. Non sempre poi la persona offesa ha prova dell'utilizzo indebito di tale casella di posta elettronica e, con esso, del realizzarsi del furto di identità ex art. 494 c.p.

B) a tale ipotesi devono essere equiparati tutti i denunciati ***accessi illegittimi ad altri account di comunicazione****, quali ad esempio chat (ipotesi frequente il sistema messanger di Microsoft denominato MSM)*

- ALTRO ACCESSO ABUSIVO

QUALIFICAZIONE GIURIDICA*: 615-ter c.p.*

FENOMENO*:*

[31] Quanto a eBay.

[32] Tali istituti infatti sono a richiedere all'utente (che, solo fittiziamente, risulta aver operato una vendita online ma in realtà si è visto artatamente rubato il proprio account) il costo della intermediazione, come da contratto che regola il commercio elettronico a mezzo della piattaforma.

1) trattasi delle vere e proprie intrusioni informatiche, spesso denunciate da società o gestori di siti web/sistemi di comunicazione

2) sempre più spesso si registrano episodi ***di violazioni di centralini telefonici VOIP[33],*** *spesso denunciate da società, di frequente compiute nei fine settimana, che permettono l'effettuazione in frode di traffico telefonico diretto a telefoni cellulari con profilo di autoricarica, numerazioni estere e satellitari o a codici a valore aggiunto* ***(e quindi trattasi anche di ipotesi ex art. 640-ter c.p.p.)***

A volte la causa dell'uso fraudolento del sistema telefonico è da rilevarsi in una falla aperta nell'infrastruttura (vulnerabilità dei firewall aziendali, bug o errate configurazioni dei sistema VoIP, previsione di password di accesso non robuste o impostate di default dal costruttore), che è sfruttata per l'instradamento del traffico telefonico.

Talvolta l'operatore telefonico al quale si appoggia la società per inoltrare le proprie telefonate, si accorge del traffico anomalo generato e blocca le chiamate con destinazioni internazionali.

- TRUFFA E-BAY
- TRUFFA SU ALTRA PIATTAFORMA

QUALIFICAZIONE GIURIDICA*: art. 640 c.p.*

FENOMENO*:*

A) Gli utenti si accordano, tramite servizi di commercio online (in particolare eBay[34]), per vendere ed acquistare della merce, prevedendo come modalità di pagamento

• il trasferimento di denaro tramite Western Union/Money Gram,
• l'uso di vaglia online,
• l'effettuazione di ricariche di carte di credito prepagate (ad esempio Postepay)
• altri sistemi di pagamento elettronico (es. paypal)

B) Molto diffuso anche l'utilizzo di assegni circolari falsi (molto spesso stranieri): tale tipologia di truffa è inizialmente emersa soprattutto in relazione alla piattaforma di secondamano.it, le cui modalità sono peraltro segnalate agli utenti dal relativo sito:

[33] Con telecomunicazioni in **Voice over IP** (*Voce tramite protocollo Internet*), acronimo **VoIP**, si intende una tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet o un'altra rete dedicata che utilizza il protocollo IP senza connessione per il trasporto dati (tratto da Wikipedia).
[34] Si noti come tale piattaforma di commercio elettronico, allo stato, accetti solo come modalità di pagamento quelle legate a ricariche postepay o tramite paypal.

OFFERTA DI PAGAMENTO SUPERIORE AL PREZZO DEL BENE VENDUTO

La truffa comincia con la ricezione di una mail, da parte di un ipotetico acquirente, interessato al prodotto che vorresti vendere. Si tratta generalmente di un acquirente che vive all'estero e che ti pagherà con un assegno. Generalmente il presunto acquirente ha molta fretta di acquistare l'oggetto e dice di avere un contatto in Italia che verrà a prendere il prodotto dove preferisci. In certi casi potrebbe offrirti due o tre volte la cifra da te richiesta a garanzia, e che potrai restituirgli la differenza alla ricezione del bene. Altre volte, potrebbe tentare di convincerti che l'assegno che ti invierà ha un importo maggiore perché parte di esso serve a sbrigare pratiche doganali o cose del genere. Quello che invece è certo è che se il bene, ad esempio, costa 2.000 euro e il presunto acquirente ti invia un assegno da 6.000 euro, ti chiederà senz'altro di inviargli la differenza. Attenzione perché la banca può accettare l'assegno e impiegare settimane prima di comunicarti che invece non è regolare e che tu hai inviato denaro a un'organizzazione criminale. Altre truffe simili nascono dall'utilizzo di ricevute di bonifico online falsificate o in caso di venditori che raccomandano un servizio di deposito a garanzia sconosciuto.

- BONIFICO/RICARICA DISCONOSCIUTA (PHISHING)

***QUALIFICAZIONE GIURIDICA**: art. 110, 640, 648 c.p.*

FENOMENO:

In tali casi la persona offesa si lamenta della fraudolenta captazione - tramite la già indicata tecnica del phishing - di informazioni e dati riservati relativi a:

- *carte di credito*
- *carte ricaricabili (es. postepay)*
- *conti correnti online*

con relativo utilizzo illecito, ad opera di terzi, tramite operazioni online idonee a privarlo di ingenti somme di denaro.

- RICICLAGGIO ELETTRONICO PROVENTI ILLECITI (CYBERLAUNDERING)

***QUALIFICAZIONE GIURIDICA**: art. 648, 648-bis c.p.*

FENOMENO:

Gli esiti delle indagini condotte fin dal 2005 dalla Procura di Milano in relazione al fenomeno del cd. phishing che ha interessato numerosi istituti di credito italiani hanno evidenziato:

- una serie di soggetti italiani che, previa precedente comunicazione delle loro coordinate bancarie a soggetti di regola tutti operanti dall'estero, si rendevano disponibili a prelevare in contanti somme di denaro fatte confluire sui loro conti a seguito di bonifici online;

- una serie di soggetti, spesso residenti in paesi dell'Est Europa, che risultavano beneficiari di somme di denaro fatte loro pervenire, tramite trasferimenti WESTERN UNION e/o MONEY GRAM da parte degli stessi soggetti italiani di cui sopra;

Tali bonifici online sono stati effettuati, in danno degli ignari titolari dei rispettivi conti ordinanti, previa illecita acquisizione delle rispettive credenziali (username e password, necessarie per le relative operazioni di home banking);

I titolari dei conti correnti italiani (cd. financial manager[35]) beneficiari di tali bonifici online, ritenendo di ottemperare ad un contratto di lavoro[36], trattengono una percentuale di quanto a loro indebitamente accreditato e trasferiscono la residua somma a persone prevalentemente residenti nei paesi dell'Est Europa con le modalità sopra indicate.

- CARTE CREDITO

QUALIFICAZIONE GIURIDICA: *art. 55 comma 9 D.lvo 21 novembre 2007, n. 231[37]*

FENOMENO:

1) nella maggior parte dei casi la persona offesa disconosce alcuni pagamenti, effettati a sua insaputa.

2) capita spesso che la Polizia Giudiziaria intervenga nei pressi di istituti di credito o di sportelli bancomat. Solamente laddove gli indagati siano trovati nel materiale possesso di carte di credito sarà possibile invocare l'art. 55 comma 9 d.lvo 231/2007 al

[35] L'intermediazione dei *financial manager* (operatore finanziario) si rende necessaria perché il sistema di home banking italiano non consente bonifici verso l'estero se non a seguito di specifici controlli ulteriori che farebbero venire allo scoperto la truffa

[36] Si noti come il Tribunale di Milano ed altri Giudici in Italia hanno tuttavia già emesso importanti sentenze di condanna nei confronti di tali soggetti, ritenendo sussistente la consapevolezza della provenienza illecita delle somme.

[37] Ove dalla lettura degli atti emerga come accertato unicamente l'avvenuto utilizzo indebito di una carta, il fascicolo deve essere iscritto solo per tale reato e non anche per l'art. 640-ter c.p.: sul punto anche provvedimento Procura Generale della Repubblica presso Corte di Appello di Milano, 1/10 Reg. contrasti, del 18.1.2010, che ha ritenuto "*interessanti ipotesi… e non idonee a determinare la competenza*" le considerazioni circa un precedente accesso abusivo al sistema informatico del correntista/possessore della carta di credito o di una frode informatica ex art. 640-ter c.p. ai suoi danni.

fine dell'arresto nella flagranza del reato[38].

- DIFFAMAZIONE ONLINE

QUALIFICAZIONE GIURIDICA: *art. 595 comma 3 c.p.*

FENOMENO: *la persona offesa lamenta una pubblicazione sulla rete internet (sito Internet, blog, forum online) lesiva del proprio onore/reputazione.*

Quanto agli altri fenomeni più marginali (e-mail o SMS diffamatori), gli stessi non rientrano tra i fascicoli assegnati al pool reati informatici e quindi non verranno trattati nel proseguo.

- ALTRO REATO INFORMATICO COME DA RE.GE.

Ove un fatto di reato non rientri nelle categorie precedentemente illustrate, e sempre che non si tratti di reato attinente la pedopornografia online *(in relazione sussiste sempre la competenza distrettuale della Procura di Milano ex l. 48/2008), occorrerà individuare la* ***corretta qualificazione giuridica*** *tra le seguenti qui riportate:*

art. 615-quater c.p. (detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)

art. 615-quinquies c.p. (diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico)

art. 617-bis c.p.(installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche)

art. 617-ter c.p.(falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche)

art. 617-quater c.p.(intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)

art. 617-quinquies c.p.(installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche)

art. 617-sexies c.p.(falsificazione, alterazione o soppressione del contenuto di

[38] Lo stesso varrà, anche se tuttavia è ipotesi di difficile verificazione, ove siano ritrovate persone nell'atto di falsificare carte di credito o nell'atto di cedere/acquisire carte contraffatte.

comunicazioni informatiche o telematiche)

art. 635-bis c.p.(danneggiamento di informazioni, dati e programmi informatici)

art. 635-ter c.p.(danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da un altro ente pubblico o comunque di pubblica utilità)

art. 635-quater c.p. (danneggiamento di sistemi informatici e telematici)

art. 635-quinquies c.p. (danneggiamento di sistemi informatici e telematici di pubblica utilità)

art. 640-quinquies c.p. (frode informatica del soggetto che presta servizi di certificazione di firma elettronica)

Si tratta, in ogni caso, di ipotesi residuali, allo stato di scarsa verificazione.

Tale classificazione è poi successivamente confluita nelle Direttive per la Polizia Giudiziaria sui primi accertamenti investigativi in materia di reati informatici. Anche qui ne riportiamo una sintesi a miglior chiarimento.

6. LE DIRETTIVE PER LA POLIZIA GIUDIZIARIA SUI PRIMI ACCERTAMENTI INVESTIGATIVI IN MATERIA DI REATI INFORMATICI E MODALITÀ DI TRASMISSIONE DELLE RELATIVE COMUNICAZIONI DI NOTIZIA DI REATO ALLA PROCURA DI MILANO

All'esito della elaborazione della classificazione "esperienziale" sopra esemplificata, una ulteriore riflessione è seguita: alla luce dell'aumento costante dei reati informatici, che vedono molto spesso un terreno fertile nella scarsa informazione dei cittadini, per la stessa Autorità Giudiziaria territorialmente competente diventa più che ragionevole ipotizzare veri e propri protocolli investigativi con le Forze dell'Ordine deputate alla ricezione della *notitia criminis*.

Il senso di simili protocolli investigativi è evidente: solo le informazioni *adeguatamente* raccolte e *prontamente* comunicate, in maniera strutturata ed organizzata, all' Autorità Giudiziaria territorialmente competente portano a risultati investigativi congrui.

A titolo di esempio, alla fine del 2004 si concretizzò – su accordo tra i magistrati del *pool* reati informatici della Procura di Milano e la Polizia Postale

di Milano - un protocollo d'intesa in relazione alle cd. truffe a mezzo *dialer*, volto altresì a richiedere alla persona offesa informazioni utili al proseguo indagini fin dal momento della ricezione della denuncia[39].

In particolare venne predisposto un apposito modulo volto a richiedere alla persona offesa le seguenti informazioni, relative all'epoca dei fatti:

- se è presente un computer in casa;
- chi adopera il pc (in modo esclusivo e residuale);
- quanti sono i componenti della famiglia;
- con quale provider ha il collegamento a Internet e quale è il numero del collegamento;
- che tipo di linea telefonica si adopera;
- quale sistema operativo utilizza e con quale cadenza viene aggiornato;
- quale antivirus utilizza;
- se il gestore telefonico ha avvisato l'utente per il traffico inconsueto e quando tale informazione è arrivata;
- se durante la navigazione si sono aperte finestre o pop-up e normalmente quali operazioni effettua per chiuderle;
- se il denunciante ha mai sentito il modem sconnettersi e ricomporre il numero durante la navigazione; in tal caso se ricorda i siti dove stava navigando ed il periodo dei fatti;
- se ha fatto analizzare il pc da persone tecniche competenti ed eventualmente quali prove a sostegno del traffico anomalo sono emerse;
- se il pc è stato formattato;
- se il denunciante è in grado si fornire copia dei dati presenti sulla directory "Download Program Files";
- se legge attentamente le finestre mostrate durante la navigazione in Internet.

Un elenco piuttosto puntuale, come si vede. Nello stesso tempo, venne predisposta una dettagliata comunicazione informativa da consegnare al denunciante. Gli scopi erano più d'uno, tra i più importanti: prevenire il verificarsi di ulteriori connessioni telefoniche non riconosciute dall'utente; fornire alla vittima ogni informazione utile sul fenomeno illecito; fornire indicazioni pratiche, utili a restituire alla Polizia Giudiziaria, su apposito

[39] Si consideri la altrimenti impossibilità tecnica, una volta acquisita la notizia di reato, di raccogliere ulteriori elementi di prova dell'intento truffaldino perseguito da chi immette in Internet i *dialer*, in assenza del computer su cui risiede il software da sottoporre a consulenza tecnica, per non dire dei lunghi tempi di risposta dei gestori telefonici coinvolti

supporto informatico, la copia dei dati presenti nella directory "*Download Program Files*"; illustrare le procedure extragiudiziali volte al recupero delle somme disconosciute, ove le relative bollette telefoniche fossero state già pagate.

All'epoca, il fenomeno dei *dialer* sembrava inarrestabile…. fu anche merito della procedura di lavoro individuata se si arrivò in breve a significativi risultati.

È ripensando a quella esperienza, e dopo aver "codificato" la ricordata classificazione dei fenomeni di reato, che è apparsa chiara l'utilità di estenderla a tutta la materia del *cybercrime.*

Nel maggio del 2011 si è così arrivati alla formalizzazione[40] (e alla successiva diffusione sotto forma di Direttive[41]) 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*".

A questo punto si comprenderà meglio perché il richiamato documento[42] è da intendersi come contributo, allo stato dell'arte, per la sistematizzazione e la razionalizzazione delle attività di indagine penale negli ambiti della criminalità informatica.

La struttura dell'elaborato, così come indicato nelle sue premesse, è quindi la seguente:

*I) una **parte generale** ricomprendente alcune informazioni di base e riferimenti fattuali/ giuridici utili per gli accertamenti di PG richiesti;*

*II) una parte relativa alla **modalità di trasmissione** della comunicazione di notizia di reato (CNR), con illustrazione*

[40] In collaborazione con il Compartimento della Polizia Postale e delle Comunicazioni di Milano e grazie alla sensibilità dimostrata dal Dirigente Salvatore La Barbera, nonché da Fabiola Treffiletti, Lisa Di Berardino, Maurizio Gatti e dal Personale addetto ai settori specializzati investigativi e tecnici.
Quanto alla Procura di Milano, il gruppo di lavoro che ha portato alla stesura finale del documento (con testi a cura di Francesco Cajani, Davide D'Agostino, Paolo De Feo, Alberto Nobili e Walter Vannini) era composto da Giuseppe Acacia, Massimiliano Carducci, Beniamino Carriero, Fabio Cavallo, Giovanni Depedro, Elisa Moretti, Elio Ramondini, Stefano Toscano ed Andrea Venturini.

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

[42] Oltre ad una versione riservata destinata alla Polizia Giudiziaria del Distretto di Corte di Appello, è stata recentemente elaborata una versione pubblica.

*a) della **scheda di accompagnamento** (che dovrà essere compilata sostituendosi al modello ottico, salvo mantenerne i riferimenti progressivi numerici) della CNR,*

*b) delle **tipologie di reati informatici,** con indicazione per ciascuna di esse delle seguenti informazioni:*

*- **QUALIFICAZIONE GIURIDICA** da attribuire ai fatti di reato,*

*- descrizione del **FENOMENO**,*

*- **PREGRESSE ESPERIENZE INVESTIGATIVE**, con indicazione degli accertamenti investigativi che di regola non sono stati in grado di restituire dati utili per il proseguo delle indagini,*

*- **ACCERTAMENTI MINIMI RICHIESTI** alla Polizia Giudiziaria che ha raccolto la notitia criminis.*

*III) un **approfondimento tecnico** su alcuni accertamenti di base*

*IV) un elenco di **riferimenti utili** (telefoni, fax, altre informazioni) per la Polizia Giudiziaria*

La redazione del documento, è importante ricordarlo, è stata motivata da ragioni contingenti e da ragioni di prospettiva.

Le ragioni contingenti attengono alla necessità di sopravvivenza dell'Ufficio del Pubblico Ministero e delle forze di Polizia Giudiziaria – alla luce della distrettualizzazione *ex* legge 48/2008 - rispetto alla crescente attività criminale basata sull'utilizzo pervasivo dello strumento informatico[43].

Le ragioni di prospettiva poi, o strategiche, rendono evidente la necessità di riflettere su alcuni punti fermi, non solo strettamente tecnici ma anche culturali con l'integrazione di saperi differenti, e di prendersi un tempo corale - dentro l'Istituzione - per riflettere sulle tendenze e contenuti dei comportamenti criminali ma, allo stesso tempo, sulla possibilità di meglio tutelare le vittime e gli interessi della collettività a cui siamo istituzionalmente demandati.

Per quanto detto sopra, tale lavoro è inevitabilmente mai concluso: per la natura dei contenuti trattati; per la mobilità delle tecniche e della interpretazione

[43] Seppure non si sia ancora ai livelli dello Stato del Michigan (G. GOGOLIN, *The Digital Crime Tsunami*, in *Digital Investigation*, 7, 2010, 3-8), certo l'insieme delle attività che costituiscono illecito penale è sempre più realizzato con l'utilizzo della risorsa informatica almeno per parti importanti, comunque costitutive del fatto reato. Cfr. sul punto G. ZICCARDI, *Investigazioni digitali e informatica giuridica*, prolusione presentata in occasione del convegno *Criminalità informatica ed accertamento penale,* Padova, 2 luglio 2011 - Atti non pubblicati.

procedurale delle norme in essere; per il riguardare essenzialmente fatti di reato che sono sempre ai confini delle competenze tecniche e delle possibilità di contrasto disponibili.

Indicare alla Polizia Giudiziaria una serie di Direttive tuttavia poteva sembrare riduttivo se non contestualmente accompagnato da una doverosa presa in carico del bisogno formativo di cui necessita ogni professione, a maggior ragione se ad altro valore tecnico e culturale aggiunto.

7. L'AGGIORNAMENTO PROFESSIONALE PER LA POLIZIA GIUDIZIARIA

Proprio dalle riflessioni sulle difficoltà in senso ampio del lavoro di contrasto alla criminalità informatica, sul ruolo della vittima e sulla possibilità di offrire ad essa una miglior considerazione e tutela, è apparso intuitivo ragionare su quali Istituzioni avrebbero avuto un interesse primario nel cooperare. L'Ente locale, non fosse che per ragioni di prossimità, è di regola il più interessato. Del resto ci sono più modi in cui Istituzioni come una Amministrazione comunale e la Magistratura possono cooperare.

Uno delle forme più immediate consiste nello scambio di competenze ed utilità. Una cooperazione istituzionale virtuosa, di reciproca soddisfazione, relativamente ad interessi condivisi.

In un periodo di severa scarsità delle risorse (ma non è sempre stato così per certi ruoli di spesa pubblica?), argomenti come la formazione alta, l'aggiornamento tecnico-professionale specialistico, il contrasto efficace alla criminalità, la tutela del mercato e della persona, risparmiatore, genitore di minore, consumatore, eccetera, si possono trovare percorsi di reciproca soddisfazione.

Vi sono risorse che permangono indipendentemente dalle difficoltà economiche: i saperi accumulati, le competenze professionali ancora attuali, i luoghi della formazione e le metodologie dell'apprendimento. Certo si tratta di garantire standard adeguati, ma la competenza non manca ed è tradizionalmente sottoutilizzata nei periodi di crisi economica.

Da queste ed altre considerazioni è nata un'ipotesi di lavoro, in parte ancora allo studio, in parte già in corso, tra il Comune di Milano - Settore Lavoro e occupazione e ricerca universitaria e la Procura di Milano - *pool* reati informatici.

L'accordo prende le mosse da un bilancio di bisogni e di vincoli oggettivi e dal rilevare che parte del problema può essere risolto con una offerta formativa utile al distretto di Corte di Appello del Tribunale milanese. Sommariamente, dal lato

della Procura di Milano le innovazioni di cui alla legge 48/08 hanno comportato l'incremento dei carichi di lavoro di cui si è già detto, e la conseguenza concreta, il bisogno, di sviluppare tecniche efficaci di comunicazione per illustrare nuove prassi investigative in corpi di Polizia Giudiziaria dalla tradizione e mandato istituzionale differenti.

Allo stesso modo, sono divenuti rilevanti gli aspetti di gestione informatica dei casi, posto il grande interesse investigativo nel discriminare il più precocemente possibile le vicende riconducibili a comportamenti criminali seriali dagli eventi episodici, e dunque una impostazione del trattamento delle basi dati relative ai fascicoli che facesse emergere le ricorrenze, gli indicatori cui porre attenzione.

Non ultimo, i fenomeni criminali inerenti l'utilizzo dell'informatica riportano normalmente la compresenza di attori appartenenti a culture e paesi differenti, anche molto eterogenei tra loro, produttori o espressione intanto di emergenze culturali nuove, esito dell'incontro di culture differenti, della mobilità umana, della ubiquità intrinseca allo strumento informatico;

Dal lato del Comune di Milano esisteva un interesse ovvio, non fosse altro che per ragioni istituzionali, al tema della vittima, alla tutela della quota più esposta della propria popolazione, da attività malevole, e – naturalmente - alla riduzione dei fenomeni di turbamento dei mercati[44].

L'accordo, poste queste premesse, si è concretizzato in più azioni, alcune ancora in fase di progetto, altre in corso di realizzazione. Tra queste, il piano formativo è forse, per tasso di innovazione, la attività più complessa.

Il piano formativo è basato sulla realizzazione di incontri secondo le forme più tradizionali dell'apprendimento: seminari, workshop e lezioni frontali, ma principalmente è fondato sulla realizzazione di una piattaforma didattica per la Formazione a Distanza (FAD) e della relativa metodologia didattica, grazie

[44] "Oggi molti scambi economici avvengono attraverso l'ausilio di piattaforme informatiche e sono in aumento i reati e le frodi connesse. Imprese e cittadini sono ugualmente colpiti. Le imprese, in particolare, sono soggette a danni significativi e perdita di fiducia negli strumenti informatici. Per questo abbiamo deciso di approfondire e dare concretezza a una collaborazione già esistente. Solo con un'efficace collaborazione tra istituzioni è possibile dare risposte serie alle imprese e ai cittadini che ci chiedono più sicurezza e informazione per prevenire i reati informatici. Con la Procura stiamo infatti costruendo anche momenti informativi per spiegare a cittadini e imprese come difendersi": così Cristina Tajani, Assessore Politiche del Lavoro, Sviluppo economico e Università del Comune di Milano, ha commentato la partnership con la Procura della Repubblica.
Il protocollo d'intesa tra Procura milanese ed Ente Locale è stato concretizzato e firmato rispettivamente da Alberto Nobili (Procuratore Aggiunto e coordinatore *pool* reati informatici) e Walter Cavalieri (Direttore centrale del Settore Politiche del Lavoro, Sviluppo economico e Università).

anche ad una convenzione in essere con il CILEA[45] che fornisce il necessario supporto tecnico informatico.

Un aspetto assolutamente originale del piano didattico è inoltre l'introduzione di materie formative di non stretta attinenza alle competenze tecnico investigative, ma pertinenti alla comprensione dei contesti sociali, culturali, antropologici e degli aspetti psicologici e criminologici dei fenomeni criminali di interesse, e della vittima.

Il piano formativo prevede il coinvolgimento attivo di attori istituzionali qualificati: Polizia dello Stato, Carabinieri, Guardia di Finanza, Polizia Locale del Comune di Milano; il coinvolgimento attivo di Cattedre universitarie delle materie forensi e delle materie non giuridiche interessate[46]; la collaborazione privilegiata con IISFA e con UNICRI[47]; l'interlocuzione attiva con i più importanti operatori privati di servizi avanzati e di mercato.

L'offerta, ad accesso assolutamente riservato, indirizzata elettivamente agli Ufficiali ed Agenti di Polizia Giudiziaria del territorio, inclusa quindi la Polizia Locale, ha un bacino teorico di oltre 1000 interessati alla formazione[48].

Allo stato, l'offerta didattica è in fase operativa. Un primo ciclo formativo, attestato dai due enti organizzatori, Procura della Repubblica e Comune di Milano, si è svolto con tre incontri in forma di seminari e lezioni frontali che si sono tenuti presso l'Aula Magna del Tribunale di Milano, a cavallo dei mesi di giugno e luglio scorso, con la presenza media di circa 400 utenti per sessione. Co-gestito con il centro di formazione del Comune di Milano di v.le D'Annunzio ed incentrato su aspetti tecnico forensi ed economici, ha avuto come docenti magistrati, referenti delle imprese internazionali afferenti i circuiti del credito e della moneta e i principali fornitori internazionali di servizi in rete.

Dopo l'illustrazione puntale delle Direttive da parte dei magistrati componenti del *pool* reati informatici, gli incontri hanno affrontato i temi relativi agli *Internet Service Providers* stranieri operanti in Italia nonché ai vari servizi di *money trasfert* e commercio elettronico.

Il proposito dichiarato è stato quello di dare spazio agli attori principali i quali, gioco forza, si trovano ad affrontare, su posizioni e con prospettive

[45] Consorzio Interuniversitario Lombardo per l'Elaborazione Automatica: *www.cilea.it.*

[46] Al momento della chiusura redazionale del presente articolo, contributi per la FAD sono in corso di elaborazione da parte di Cattedre delle Università milanesi (Statale, Bicocca, Bocconi) nonché del Dipartimento di Matematica e Informatica della Università di Catania. Sono in corso contatti con altre Cattedre per le materie non giuridiche.

[47] *United Nations Interregional Crime and justice Research Institute: www.unicri.it.*

[48] Alla scorsa settimana, le pre-iscrizioni al corso a distanza erano 250. La data di chiusura delle iscrizioni è prevista per la fine di febbraio 2012: cfr. *http://www.procura.milano.giustizia.it/formazione-per-la-polizia-giudiziaria.html.*

diverse ovviamente, le medesime problematiche della Polizia giudiziaria in materia di reati informatici.

In particolare si è voluto creare un momento di incontro tra *law enforcement* e i responsabili dell'offerta informatica, dei *social network,* dei *provider* di servizi, affinché questi ultimi potessero avere a disposizione uno spazio adeguato per rappresentare le *policy* adottate al fine di ottemperare alle richieste delle Autorità Giudiziaria in materia di contrasto ai reati, ed in particolare quelli informatici nonché attinenti al riciclaggio di moneta elettronica. E di illustrazione, al fine della reciproca comprensione, fuori dalla contingenza dell'indagine penale, dei propri interessi e logiche di azione.

I temi trattati negli incontri[49], oltre ad illustrare le *policy* utilizzate da Facebook, Google, Yahoo! e Microsoft, hanno così affrontato anche lo spinoso

[49] Nello specifico hanno partecipato:
- **American Express** nella persona del dott. Fabio LIBERATORI il quale ha illustrato tutta le tipologie di carte gestite da AE, gli strumenti interni a contrasto delle frodi e le collaborazioni con le Autorità Giudiziarie.
- **CartaSi** nelle persone del dott. Marco CORTELLARI e della dott.ssa Roberta LUCENTINI i quali hanno discusso di frodi mediante carte le carte di credito gestite dalla loro società, la storia delle truffe in parola, la collaborazione internazionale e le iniziative a contrasto sviluppate in Italia.
- **Facebook Inc.** nella persona del responsabile rapporti con l'Autorità Giudiziaria dott. Christian PERRELLA che ha illustrato le modalità di richiesta dei dati degli utenti da parte dell'Autorità Giudiziaria.
- **Google Italia s.r.l.** nella persona dell'Avv. Marco PANCINI e dell'Avv. Marco Tullio GIORDANO: sono stati fatti cenni sulla nascita del noto motore di ricerca, il suo sviluppo, i servizi offerti e le procedure per acquisire i dati degli utenti da parte dell'Autorità Giudiziaria
- **Yahoo! Italia s.r.l.** nella persona del responsabile dell'ufficio legale Avv. Federica CELORIA la quale ha rappresentato tutti i servizi forniti da Yahoo! e le relative procedure di richiesta dati da parte dell'Autorità Giudiziaria
- **MasterCard** nella persona del dott. Luca CORTI il quale ha illustrato la storia delle carte di credito, i tipi di carte gestite da MasterCard, le tipologie di transazioni consentite e le frodi scoperte.
- **Microsoft Italia s.r.l.** nelle persone del responsabile dell'ufficio legale dott.ssa Sibilla RICCIARDI, del responsabile ufficio Antipiracy dott.ssa Silvia PIACENZA e del responsabile ufficio rapporti Autorità Giudiziaria dott.ssa Cristina MOLTENI: hanno illustrato i servizi Microsoft e le *policy* aziendali in materia di rapporti con l'autorità Giudiziaria.
- **Poste italiane S.p.A.** nelle persone del dott. Giuseppe MAZZARACO e del dott. Francesco TAVONE i quali hanno illustrato il funzionamento della banca dati riservata "PosteAG" che è a disposizione dell'Autorità Giudiziaria e della Polizia giudiziaria per le richieste dati relative ai propri clienti.
- **VISA** nella persona del dott. Joe GOMEZ il quale ha trattato l'argomento frodi illustrando, altresì, le tipologie di carte e le investigazioni a supporto delle Autorità Giudiziarie.
- **WesternUnion** nella persona dell'Avv. Paolo SINIBALDI il quale ha illustrato il servizio di *money trasfer* in generale e quello di WU in particolare nonché i le procedure per la richiesta dei dati da parte dell'Autorità Giudiziaria.

problema delle truffe su piattaforme di commercio elettronico/*phishing* con pagamenti/trasferimenti indebiti di somme di denaro tramite sistemi di *money transfert.*

In buona sostanza, l'idea di fondo è stata quella di verificare la possibilità di collaborazione puntuali, reciprocamente produttive di consapevolezza dei vincoli e delle risorse cui i rispettivi ambiti professionali afferiscono.

7.1 Il piano di formazione a distanza (FAD) per il 2012

A partire dal mese di novembre passato, in collaborazione con alcune cattedre delle Università milanesi ed i docenti del centro di formazione di v.le D'Annunzio, si sono tenute alcune lezioni frontali e *workshop*[50]; inoltre, grazie ad altre risorse messe a disposizione dal Comune di Milano (centro di formazione professionale per l' Informatica, il Terziario e i Servizi all'Impresa - sito in via Pepe), si è dato avvio ad un ciclo di incontri per l'alfabetizzazione informatica e di introduzione di primi elementi di tecniche di indagini investigative (il corpo insegnante, in questo caso, è composto – oltre che da docenti del Comune - da Ufficiali e Agenti della Polizia Postale di Milano e della Squadra di PG reati informatici della Procura).

Nei primissimi mesi del 2012 prenderà il via il corso di formazione a distanza (FAD), che è l'impegno formativo di eccellenza vero e proprio. Sarà riservato agli operanti di Polizia Giudiziaria del Distretto di Corte d'Appello di Milano ed ai magistrati, con una flessibilità modulare per la fruizione dei contenuti secondo la pregressa competenza acquisita.

---

[50] Il 2 dicembre 2011 si è tenuto all'Università degli Studi di Milano il primo incontro: il prof. Giovanni Ziccardi si è occupato della parte relativa all'etica nelle investigazioni, il prof. Pierluigi Perri delle "nuove" figure di delitti informatici dopo la legge 48/2008, il dott. Gianluca Braghò (già componente del *pool* reati informatici della Procura di Milano) e l'avv. Andrea Monti hanno affrontato i profili procedurali della l. 48/2008, il prof. Matteo Giacomo Jori ha trattato il tema delle nuove tecnologie e nuove ipotesi di violazione del diritto d'autore.
Il giorno 11 gennaio 2012 si terrà presso l'Università Milano-Bicocca il secondo incontro dal titolo "*Cenni introduttivi di Digital Forensics: aspetti tecnici e profili processuali*" (relatori: Giuseppe Vaciago, docente di Informatica Giuridica presso l'Università dell'Insubria; Mattia Epifani, *Digital Forensics Specialist*. Introdurrà i lavori il prof. Andrea Rossetti, Cattedra di Informatica Giuridica).
Infine il 7 febbraio 2012 presso l' Aula Magna del Centro di Formazione di via G. D'Annunzio 15, Milano si terrà l'incontro dal titolo "*Vittima, intorno sociale, istituzioni. Un punto di vista interdisciplinare su aspetti inusuali nelle strategie di contrasto ai computer crimes*" (docenti relatori: Maria Mormino, sociologa; Walter Vannini, sociologo criminologo; Elisa Panzetti psicoterapeuta, arte terapeuta, psicologa).

Come riporta il documento di progettazione pedagogica,

> *"... La **FAD** (**Formazione A Distanza**) utilizza le tecnologie Internet per erogare online contenuti didattici multimediali. La piattaforma e-learning (Learning Management System) sulla quale poggiano i materiali è configurata come ambiente virtuale nel quale si sviluppano insegnamento e apprendimento. Nello specifico, il corso Cybercrime verrà erogato sulla piattaforma Moodle, una piattaforma didattica open source tra le più diffuse e affidabili, orientata a progetti collaborativi.*
>
> *E' importante rilevare che questa tipologia di formazione non esclude per nulla il rapporto interpersonale, importante variabile di ogni percorso di apprendimento, al quale sono collegate motivazione, processo cognitivo, valutazione. Si parla di **apprendimento collaborativo** proprio per indicare l'apprendimento fondato sulla collaborazione: lo studente del corso e-learning non è solo, ma fa parte e si relaziona con una comunità di apprendimento, con i docenti e con il tutor (un "supervisore" del processo di apprendimento e dell'accesso/produzione di contenuti didattici).*
>
> ***(...)** La scelta della modalità di erogazione online per il corso Cybercrime offre molteplici vantaggi rispetto ad un'aula tradizionale, sia agli utenti che a chi fornisce la formazione.*
>
> *L'utente ha la libertà di fruire dei contenuti nei tempi e con le modalità preferite in armonia con le proprie esigenze, evitando la necessità di spostamenti fisici.*
>
> *Chi effettua la formazione ha diversi vantaggi: la controllabilità del processo di apprendimento, con la possibilità di **monitorare** i progressi degli allievi tramite gli strumenti di **tracciamento** che offre la piattaforma; la possibilità di aggiornamento immediato dei contenuti didattici; il contenimento dei costi e la semplificazione della logistica; il raggiungimento di utenti dislocati in differenti*

aree territoriali.

***(...)** si stanno predisponendo gli strumenti che la piattaforma offre secondo le specifiche esigenze del corso:*

- È previsto l'utilizzo di forum

- Sono stati impostati dei database per la raccolta di testi, periodici, documenti e link di interesse, con previsto accesso a sistemi bibliotecari online

- È stato creato un glossario di termini informatici che conterrà anche la pronuncia per i termini inglesi di uso più frequente.

- Sarà disponibile un'area di segnalazione eventi collegata al calendario

*Partendo dal piano di lavoro predisposto dalla Procura, i contenuti didattici, suddivisi in Moduli o Unità didattiche, saranno organizzati in **Learning Objects (Oggetti Didattici)**, unità di contenuto complete dal punto di vista didattico, centrate su un obiettivo di apprendimento, costruite privilegiando l'approccio multimediale per rafforzare l'efficacia dell'apprendimento (testo, immagini, video, audio, animazioni).*

Nello stesso modo verrà creato un percorso con contenuti di tipo "umanistico" che affiancheranno i contenuti tecnico-investigativi" [51]

Gli argomenti di interesse, in estrema sintesi, saranno[52]:

- informatica e nuove tecnologie applicate alle investigazioni (nozioni di base e/o aspetti di approfondimento)
- elementi di base sulla sicurezza informatica e protezione dei dati
- storia del diritto penale e processual penale inerente i reati informatici
- elementi di diritto penale e di procedura penale legati a
    - reati informatici previsti dal codice penale,
    - pedopornografia *online*,
    - diffamazione *online*,
    - tutela del diritto d'autore *online*,
    - truffe su piattaforme di commercio elettronico
    - *cybericiclaggio*
    - tutela dei mezzi di pagamento elettronico
- elementi di *digital forensics* (aspetti peculiari di approfondimento)
- storia ed economia del crimine informatico
- fenomenologia, forma e contenuto emergenti della comunicazione informatica
- culture e linguaggi emergenti nella sfera della comunicazione e dell'informatica
- approcci sociologici, criminologici, vittimologici ed antropologici al

[51] A. FERRARA, D. SANTALUCIA, *Il Corso on-line per Operatori della Polizia Giudiziaria denominato Cybercrime - Progetto FAD e organizzazione didattica*, *paper* interno, Milano, ottobre 2011.

[52] Cfr. *http://www.medialaws.eu/call-for-studies/.*

crimine informatico ed alla vittima del crimine informatico
- psicologia e clinica del trauma: teorie, cause, aspetti, forma, contenuto, trattamento
- pedagogia e formazione dell'adulto professionalizzato: l'*e-learning*.

8. UN SITO INTERNET INFORMATIVO PER LA CITTADINANZA E PER LA POLIZIA GIUDIZIARIA

Al fine di fornire informazioni qualificate a destinatari sempre più numerosi, è stata di pari passo creata – all'interno del sito istituzionale della Procura di Milano – una apposita area "reati informatici"[53]. Essa contiene, tra l'altro, indicazioni utili per le potenziali vittime della criminalità informatica.

Inoltre, dopo gli ultimi incontri di formazione per la Polizia Giudiziaria del Distretto, i relativi materiali[54] sono stati resi disponibili previa iscrizione ad un'area ad accesso riservato alla Polizia Giudiziaria del Distretto.[55]

Tale sezione è stata voluta, sviluppata e creata in proprio dalla Procura di Milano, avvalendosi - per la sola realizzazione tecnica di politiche di sicurezza adeguate alle informazioni di carattere confidenziale ivi contenute - di una società (Email.it s.r.l.) che ha messo a disposizione, previo contratto a titolo oneroso, un *server* dedicato a Milano ed una adeguata piattaforma per la

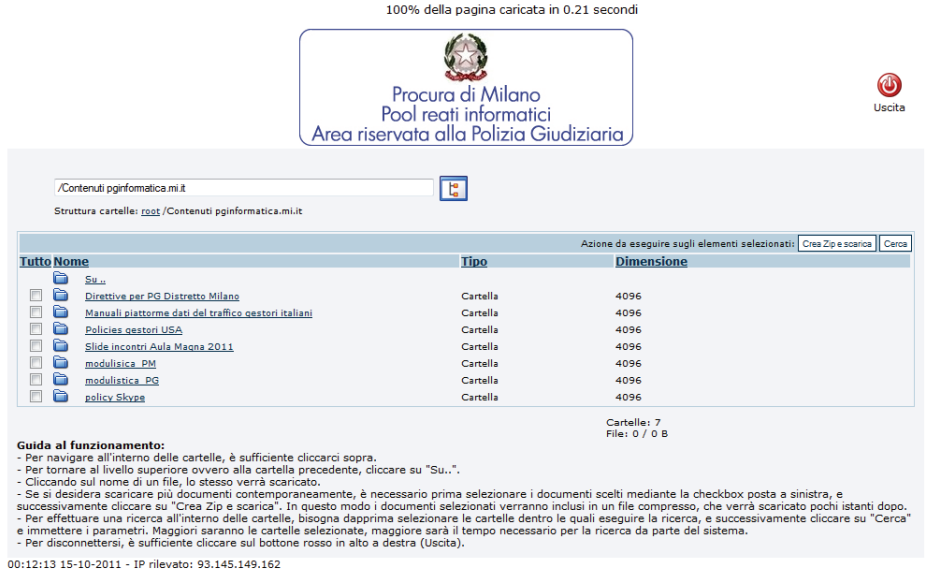
[53] Pagina raggiungibile all'indirizzo *www.procura.milano.giustizia.it/reati-informatici.html.*
[54] Alcuni materiali di interesse generale sono liberamente consultabili all'indirizzo *www.procura.milano.giustizia.it/materiali-polizia-giudiziaria.html.*
[55] Area raggiungibile dall'indirizzo *www.pginformatica-mi.it/main.html.*

gestione dei materiali e di *logging* degli accessi.

Accedi all'area riservata
alla polizia giudiziaria

Richiedi l'accesso all'area
riservata alla Polizia Giudiziaria

Una volta ottenute le credenziali di accesso, la Polizia Giudiziaria potrà beneficiare - all'interno delle varie sezioni tematiche - materiali utili e informazioni relative allo specifico settore (ad iniziare, come ricordato, dai materiali degli ultimi incontri di formazione, messi a disposizione dagli stessi relatori intervenuti).



È in progetto, altresì, di inserire all'interno dell'area riservata un *forum* di discussione nel quale tutti potranno confrontarsi – in un ambiente riservato, confidenziale – sugli argomenti che qui ci interessano.

L'importanza di tale "luogo di incontro" apparirà ovvia ai fruitori del *peer to peer* quale è la *mailing list* di IISFA: si va sempre più verso un contesto nel quale anche nelle investigazioni di tipo tradizionale ci si trova ad affrontare l'argomento "*cyber*". Invero, termini quali *log files,* comunicazioni in *VoIP, trace* di un sito internet, analisi degli *header* di un messaggio *e-mail* sono sempre più

di uso comune e, pertanto, è impensabile che tali argomenti vengano affrontati con un approccio *long life learning*, più che di "minima" preparazione di base, da parte degli operatori di Polizia Giudiziaria e della stessa Magistratura, posto che la criminalità (sia organizzata che comune) utilizza, in maniera sempre più massiva, gli strumenti che la *innovation tecnology* mette loro a disposizione.

9. UNA PROPOSTA DI LEGGE PER L'ASSEGNAZIONE ALLA POLIZIA GIUDIZIARIA DEI BENI INFORMATICI SEQUESTRATI/CONFISCATI NELLE INDAGINI INFORMATICHE

Come ci piace sempre ricordare, le nuove tecnologie costituiscono un'affascinante sfida per tutti, indipendentemente dalla prospettiva con la quale si vogliano osservare ai fini di studio: in questo ambito "guardie e ladri" si fronteggiano con intenti opposti, trasferendo gran parte della contesa in dimensioni ugualmente nuove quale il cd. *cyberspazio*.

Tuttavia, lo squilibrio tecnologico ancora esistente – quantomeno nella realtà italiana – tra dotazioni informatiche messe a disposizione alle Forze di polizia e quelle utilizzate dalla criminalità appare, allo stato, incolmabile. Basti solo citare la vicenda delle apparecchiature informatiche in uso all'intera Sezione di Polizia Giudiziaria della Procura di Milano, acquisite dal Ministero dell'Interno con provvidenze finanziarie messe a disposizione, *una tantum* e per tutte le Sezioni di Polizia Giudiziaria italiane, da una legge del 1992[56], ovvero un anno

[56] Cfr. L. FERRARELLA, *Milano, il tribunale senza 300 pc*, in Corriere della Sera, 18 novembre 2007: "*Non ci sono, né ci potranno essere, i computer necessari al lavoro dei 300 uomini della polizia giudiziaria della Procura della Repubblica di Milano. Vale per tutta Italia, ma il ministero dell' Interno ha risposto così al procuratore Manlio Minale che in estate aveva fatto proprio l' Sos lanciato dai circa 110 poliziotti, dagli altrettanti carabinieri, e dalla settantina di finanzieri che compongono la sezione di polizia giudiziaria della Procura, cioè il sistema nervoso delle indagini degli 80 pm milanesi: gli ultimi pc sono stati comprati «una tantum nel 1992», soldi non ce ne sono più stati e nemmeno ce ne saranno, quindi «spiace comunicare - conclude il Viminale - che non siamo in grado di soddisfare la richiesta di codesta Procura». La sconfortante risposta è stata messa nero su bianco dal Direttore centrale dei Servizi tecnico-logistici del Dipartimento di Pubblica sicurezza del ministero dell' Interno, il viceprefetto Giovanna Iurato, in risposta alla missiva che Minale aveva inviato in estate al dicastero di Giuliano Amato. "Le attuali dotazioni di apparecchiature tecnologiche degli uffici di polizia giudiziaria presso le Procure - spiega il Viminale - furono acquisite con le provvidenze finanziarie messe a disposizione, una tantum, dalla legge 217 del 28 febbraio 1992». Una tantum. E 15 anni fa. E pazienza se un pc sarebbe già obsoleto dopo 3/4 anni, e se distanza di 15 anni sono ovviamente tutti o rotti o difettosi. «Dopodiché - ammette il ministero -, non sono stati disposti ulteriori finanziamenti per il naturale rinnovamento. E' stato istituito solamente un capitolo di spesa per la sola gestione e manutenzione, la cui dotazione economica è appena sufficiente ad assicurare la funzionalità*

prima della Legge 23 dicembre 1993 n. 547 che – per la prima volta in Italia – introduceva nel codice penale adeguate fattispecie incriminatrici in materia di crimini informatici.

Sia concesso, per rendere meglio l'idea, riportarsi alle dotazioni[57] come

in particolare delle fotocopiatrici e del settore automobilistico». Conclusione della struttura del ministro Amato: «Pertanto, in attesa di una riforma strutturale del capitolo che consenta anche l'acquisto di apparecchiature, e di un suo congruo rifinanziamento, spiace comunicare che la scrivente (Direzione, ndr) non è in grado di soddisfare la richiesta di codesta Procura». A rigore, questo vorrebbe dire che a Milano i 300 uomini della polizia giudiziaria non potrebbero più svolgere indagini. Solo una colossale dose di ipocrisia, infatti, consente di far finta di ignorare che già adesso, in assenza di dotazioni d'ufficio, poliziotti-carabinieri-finanzieri mandano avanti la baracca soltanto perché o hanno comprato di tasca propria qualche computer (sul quale peraltro non possono utilizzare i programmi d'ufficio perché il loro caricamento non è autorizzato su pc non dell'Amministrazione), o usufruiscono di vecchi modelli in via di rottamazione concessi per poco tempo in comodato d'uso dalle società che forniscono alle forze dell'ordine i materiali per le intercettazioni telefoniche. Oppure vampirizzano a catena, finché possono, i vecchi pc dismessi dai magistrati quando alle toghe arrivano forniture più recenti. E' il fai-da-te del tirare avanti in attesa della «riforma strutturale». Che «spiace comunicare» sia ancora latitante".

[57] **"***L'attuale dotazione ufficiale di PC in carico a questa Sezione di P.G. risalente in massima parte alle forniture 1997-1999 (l'ultima fornitura di alcuni PC portatili è del 2001) è da considerarsi nella sua totalità obsoleta, inidonea agli utilizzi ordinari dei servizi di Polizia giudiziaria e, in ogni caso, quasi completamente non funzionante e posta, con regolare procedura amministrativo "in fuori uso": le pochissime attrezzature ancora parzialmente utilizzate sono in precarie condizioni e prive comunque dei requisiti minimi per l'impiego dei programmi attualmente utilizzati con finalità connesse all'attività di P.G., per l'accesso alle reti e per la garanzia di sicurezza e di conservazione dei dati, i quali com'è noto, rivestono perlopiù la qualifica di "dati sensibili" ai fini delle vigenti normative.*

Il solo materiale tecnico-informatico fornito in via ufficiale dagli Uffici ministeriali preposti e dalla TLC e tuttora in condizioni di parziale o piena efficienza -con la precisazione che le fotocopiatrici Panasonic e Canon sono fornite in uso con contratto di noleggio- consiste in:

Polizia di Stato (organico: 106 Ufficiali ed Agenti di P.G.)

Nr. 1 PC Olivetti Advalia (fornito dalla TLC come terminale telematico);
Nr. 5 stampanti laser Kjocera FS – 1020D;
Nr. 1 stampante Lexmark T522 (fornito dalla TLC)
Nr. 2 Fotocopiatrici – stampanti Panasonic DP 4520;
Nr. 2 Fotocopiatrici – stampanti Panasonic DP 3010;
Nr. 2 Fotocopiatrici Canon IR 2016;
Nr. 2 Fax Brother MFC 8220;

Carabinieri (organico: 105 Ufficiali ed Agenti di P.G.)

Nr. 5 PC portatili Olidata mod. A320T con stampante;
Nr. 1 Server Olidata Toraton (utilizzato esclusivamente come word processor)
Nr. 3 Stampanti laser Kyocera FS – 1020 D;
Nr. 1 Fax Brother MFC 8220;
Nr. 2 Fotocopiatrici – stampanti Panasonic DP 4520;
Nr. 1 Fotocopiatrice – stampanti Panasonic DP 3010;
Nr. 2 Fotocopiatrici Canon IR 2016;
materiale del tutto non funzionante e da porre in stato di "fuori uso":

da elenco recentemente trasmesso dai responsabili della Sezione di PG della Procura di Milano[58].

Date tali premesse ed anche in seguito ad una autorevole pronuncia giurisprudenziale in materia[59], come *pool* reati informatici di Milano ci si è fatti così promotori di un dibattito culturale[60] atto ad incidere in maniera positiva,

---

Nr. 5 PC portatili Olidata mod. A320 T con stampante;
Nr. 2 Telefax Olivetti OFX 3200.

Guardia di Finanza (organico: 63 Ufficiali ed Agenti di P.G.)
Nr. 2 Fotocopiatrici – stampanti Panasonic DP 4520;
Nr. 1 Fotocopiatrice – stampante Panasonic DP 3010;
Nr. 2 Fotocopiatrici Canon IR 2016.

TOTALE dotazione informatica attuale Sezione di P.G. – Procura presso Tribunale (a fronte di un organico complessivo di 274 Ufficiali ed Agenti di P.G.)
Nr. 2 PC;
Nr. 5 PC portatili;
Nr. 8 Stampanti laser Kyocera FS – 1020 D;
Nr. 1 Stampante Lexmark T522;
Nr. 10 Fotocopiatrici – stampanti Panasonic DP;
Nr. 6 Fotopiatrici Canon IR 2016;
Nr. 3 fax Brother (due richiesti in restituzione);

L'attività dell'ufficio, che da tempo versa in condizioni di assoluta emergenza in relazione alle dotazioni in argomento, come più volte segnalato, viene svolta attualmente utilizzando per un verso materiale dismesso dagli Uffici del Ministero della Giustizia e per un altro apparecchiature cedute in comodato d'uso da società che avevano in precedenza messo a disposizione detta attrezzatura per le intercettazioni telefoniche collegate alle indagini.
Con riguardo alla prima tipologia di PC, l'obsolescenza e la scarsità di tale materiale non appare in alcun modo rispondente neppure alle esigenze complessive minime della Sezione; mentre in riferimento alle (peraltro assai ridotte numericamente) attrezzature delle Società esterne menzionate, va rilevata la precarietà del titolo di possesso […].
La situazione descritta, pertanto, ha posto e pone gravi problemi di funzionalità all'attività di Polizia Giudiziaria svolta da questa Sezione".

[58] Nota del 20 settembre 2011 a firma del V.Q.A. Marco Ciacci (Responsabile Aliquota Polizia di Stato), del Ten. Col. Vito Bianco (Responsabile Aliquota Carabinieri) e del Magg. Ernesto Carile (Responsabile Aliquota Guardia di Finanza).

[59] Cfr. Giudice per le indagini preliminari presso il Tribunale di Milano, sentenza 10.12.2007 (estensore: Gamacchio) in *Rivista di Giurisprudenza ed Economia d'Azienda*, 4/2008: il Giudicante, all'esito di una analitica ricognizione normativa in materia di reati informatici che ha portato, per la prima volta nel panorama italiano, alla condanna di associazioni per delinquere di carattere transazionale sistematicamente dedite alla commissione di reati di *phishing* ai danni di correntisti italiani, disattendeva sul punto la richiesta del Pubblico Ministero (volta ad ottenere l'assegnazione dei sofisticatissimi computer portatili – utilizzati dai *phisher*s e quindi da confiscare - alla Polizia Giudiziaria procedente) "*per mancanza di previsione normativa*". *Contra*: alcune precedenti decisioni di merito, tuttavia tutte succintamente motivate sul punto.

[60] Il tema è stato discusso, tra l'altro, durante l'IISFA FORUM 2010 (Milano, 7 maggio 2010): cfr. L. FRIGERIO, *Confisca e utilizzo "sociale" per i pc degli hackers*, in *http://www.liberainformazione.org/news.php?newsid=11126.*

in una simbolica ottica deterrente, sul recente assetto normativo in materia di contrasto alla criminalità informatica.

E, idealmente quale ultimo atto della qui indicata strategia globale di contrasto, alla fine tale sforzo ha portato alla luce il disegno di legge n. 2271 recante "*Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica*"[61].

10. IN LUOGO DI UNA CONCLUSIONE

Molto di quanto è stato fatto e ancor più quel che è in divenire nasce da un bisogno urgente di adempiere ai propri doveri in condizioni oggettivamente avverse, a fronte di una scarsità di risorse materiali, di prassi che faticano a tenere il passo con il moltiplicarsi dei vincoli e di un'organizzazione poco attenta alle vittime, dove il 'poco' è esito della attenzione e diffusa sensibilità della società civile al tema.

Eppure, all'orizzonte, intravediamo un affermarsi di generazioni sensibili e preparate al lavoro nelle e con le Istituzioni, per cui il formarsi e fare ricerca è una prassi ovvia e la collaborazione una occasione di crescita professionale: un simile contesto culturale offre sollievo alla nostra quotidiana fatica di affrontare la crescente complessità della attualizzazione della legge penale alla dinamica mutevole dei fenomeni criminali e, con essa, dell'attuazione dei precetti costituzionali in materia (sia in relazione alle garanzie difensive da riconoscersi agli autori di reati informatici ma anche alle non contrapposte attese delle vittime di tali fenomeni illeciti).

Infatti, anche quando - sotto la pressione delle necessità date da scarsità di risorse e di rispetto della volontà del Legislatore - ci si occupa di fatti apparentemente distanti da indagini e reato, la Procura della Repubblica rimane al contempo interlocutore primo della vittima e dell'indagato. Allo stesso tempo, l'aggiornamento professionale degli operatori di Polizia Giudiziaria risulta complessivamente strategica perché essi stessi, pur trovandosi spesso ad operare con entrambi i protagonisti del crimine informatico, per primi avvertono la necessità di un supporto formativo specifico.

In tale ottica le Direttive, nel razionalizzare l'organizzazione interna del lavoro, delimitano qualità e quantità delle ingerenze nella vita privata

[61] D'iniziativa dei Senatori Casson, Bianco, D'Ambrosio, Chiurazzi, De Sena, Galperti, Garraffa, Incostante e Maritati (comunicato alla Presidenza il 12 luglio 2010). Il testo del disegno di legge è reperibile su *http://www.senato.it/service/PDF/PDFServer/BGT/00502184.pdf*. La scheda dei lavori al Senato è consultabile a partire da *http://www.senato.it/leg/16/BGT/Schede/Ddliter/35646.htm*. Il testo è stato approvato definitivamente il 7 febbraio 2012.

dell'indagato anche attraverso una migliore, ed omogenea per ogni corpo di Polizia Giudiziaria, prassi investigativa definita secondo tipo e complessità del reato. Esse inoltre invitano le imprese e la cittadinanza ad una miglior collaborazione e minor diffidenza verso la pubblicità dei fatti reato, favorendo la conoscenza *ex ante* delle modalità operative della forze di Polizia Giudiziaria e delle circostanze di fatto che, se prontamente riferite, sono utili per il prosieguo delle indagini.