Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea

Information Technologies in the criminal investigation: a European perspective

a cura di Francesco Cajani – Gerardo Costabile

experta edizioni

Il presente volume è pubblicato con il contributo dell'UAE e di IISFA
e senza alcuna finalità di lucro.

Experta S.r.l.
Corso della Repubblica 144, 47121 Forlì
Tel. 0543.370355 - Fax 0543.33769
www.experta.it - info@experta.it

SOMMARIO

Introduzione 9

A) Gli attori
The parties

1. M. CARDUCCI, La cooperazione giudiziaria e di polizia nelle indagini sul cybercrime: l'esperienza del pool reati informatici presso la Procura della Repubblica di Milano. 13
2. Gli organismi di coordinamento giudiziario ed investigativo a livello europeo 25
3. A. SEGER, *The "Budapest" Convention on Cybercrime and criminal money on the Internet* 31
4. I punti di contatto nazionali (Rete 24/7) 37
5. F. VAN LEEUW, *Cybercrime vs. law enforcement: the urgent need for new ways in the international cooperation. Some practical examples* 41

B) Le tracce informatiche: individuazione, conservazione e loro acquisizione
Investigation and examination of digital evidence

1. S. ATERNO, *Data retention*: problematiche giuridiche e prospettive europee 55
2. F. CAJANI, *Cloud computing, data protection, data retention: Business vs. Law, US vs. Europe*. 101
3. G. COSTABILE, *Computer forensics* e informatica investigativa: profili tecnici di base 123
4. D. GABRINI, *Live Forensics* e *Cloud Computing*: due frontiere delle indagini digitali 139
5. G. LATTANZI, La legge 48/2008 e i primi interventi della Corte di Cassazione in materia di sequestri informatici 155
6. S. MASON, *The European overview on computer seizures* 163

***C)* Linee guida e *best practice* negli accertamenti informatici**
Guidelines and best practice in the computer crime investigations

1. G. COSTABILE - G. CINGOLANI, Analisi tecnico-giuridica sulle indagini informatiche e la *computer forensics* in Europa [ottobre 2007 / gennaio 2008] 171
2. L. LUPARIA - G. ZICCARDI, Le "migliori pratiche" nelle investigazioni informatiche: brevi considerazioni sull'esperienza italiana 211
3. Le linee guida di cooperazione tra le Forze di Polizia e gli *Internet Service Providers* elaborate nell'ambito del Consiglio d'Europa 221
4. F. CAJANI, La destinazione dei beni informatici e telematici sequestrati o confiscati: spunti per una modifica normativa in tema di contrasto al *cybercrime* 225

D) Appendice
Appendix

1. *Convention on Cybercrime* 243
2. *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime* 281
3. *Eurojust strategic meeting on "cybercrime" (Athens, 23-24 October 2008)* 291
4. *Investigation, Prosecution and Judgment of Information Technology Crime: legal framework and criminal policy in the European Union (Durbuy, 25-28 November 2008)* 295
a- F. VAN LEEUW, *Working report* 298
b- *Simple case* 313
5. S. VACARU, *Criminal pursuit in the romanian case of cyber crime offences* 317

6. IISFA - *Information Systems Forensics Association, Italian Chapter* 339
7. CSDPE - *Centro Studi di diritto penale europeo - Institute for Research into European Criminal Law* 343

1. La cooperazione giudiziaria e di polizia nelle indagini sul *cybercrime*: l'esperienza del pool reati informatici presso la Procura della Repubblica di Milano.

Massimiliano CARDUCCI[1]

SOMMARIO: 1. Il pool reati informatici della Procura della Repubblica di Milano - 2. La cooperazione giudiziaria nelle indagini internazionali in materia di cyber crime - 2.1. Le Convenzioni del Consiglio d'Europa - 2.1.1. La convenzione di Bruxelles del 29 marzo 2000 sull'assistenza giudiziaria in materia penale - 2.1.2. La Convenzione di Budapest del 23 novembre 2001 sul cyber crime -2.2. La necessità dell'armonizzazione dei sistemi penali e degli indirizzi di politica criminale - 2.3. La cooperazione giudiziaria nelle indagini internazionali in materia di cybercrime.

[1] Sostituto Procuratore della Repubblica presso il Tribunale Ordinario di Milano – pool reati informatici

1. Il pool reati informatici della Procura della Repubblica di Milano

L'idea di creare un gruppo di magistrati del Pubblico Ministero presso la Procura della Repubblica di Milano, specializzati nella materia dei reati informatici, nacque all'indomani dell'entrata in vigore della L. n.547/93, che introdusse nel codice penale italiano i reati informatici in senso stretto, nella prospettiva di dover far fronte ad un numero elevato di procedimenti scaturiti da innumerevoli denunce e querele finalizzate a perseguire questo tipo di illecito penale.
Per la verità, all'epoca fu destinato a tale specializzazione un solo magistrato[2], con il quale collaborarono esclusivamente forze di Polizia Giudiziaria esterna, segnatamente appartenenti alla Polizia Postale, anche perché non vi era alcuna competenza da parte degli agenti ed ufficiali di Polizia Giudiziaria della Sezione presso la Procura della Repubblica.
Comunque, quella che già in quegli anni si riteneva che sarebbe stata la nuova ed assai problematica frontiera della criminalità, invero, non si è rivelata tale, perché i procedimenti penali iscritti dalla Procura della Repubblica di Milano negli anni novanta sono stati molto pochi, quelli con indagati compiutamente identificati addirittura nell'ordine di qualche decina e concernenti quasi esclusivamente il delitto di accesso abusivo ai sistemi informatici di talune biblioteche comunali.
Le ragioni di tale, inaspettato, scarso flusso di notizie di reato fu dovuta essenzialmente al fatto che tutto sommato ci si trovava di fronte ad una novità assoluta: l'uso di internet era ancora poco più che una curiosità, un hobby, ed i mezzi e gli strumenti di navigazione erano ancora estremamente lenti e comunque decisamente costosi. Ma soprattutto non si sporgeva denuncia: le persone fisiche private, parti lese o danneggiate dai reati, erano marginalmente interessate dal fenomeno, mentre le persone giuridiche private (banche, assicurazioni, ed altro) "preferivano" ingaggiare una competizione personale con l'hacker o semplicemente potenziare le proprie misure di protezione e di sicurezza dei sistemi informatici piuttosto che affidarsi alla Autorità Giudiziaria ed alle Forze di Polizia.
Lo scenario cambia radicalmente con l'avvento del terzo millennio, quando il numero di reati informatici denunciati o comunque portati all'attenzione dell'Autorità Giudiziaria cresce in modo esponenziale.
Dopo un attento monitoraggio del flusso dei reati informatici denunciati (accesso illegale ai sistemi informatici attraverso atti di pirateria, intercettazioni illegittime, frodi varie ai danni degli utenti, spionaggio e/o sabotaggio dei sistemi, frodi realizzate attraverso la clonazione di carte di credito, bancomat o altri mezzi di pagamento, truffe commerciali *online*, vari tipi di contraffazione

[2] Si tratta del dr. Marco Maria Alma.

realizzati tramite il computer, pornografia minorile, incitamento, istigazione o trasmissione di istruzioni relative alla realizzazione dei più svariati crimini tradizionali, molestie informatiche (il c.d. *cyberstalking*), gioco d'azzardo *on line*, prostituzione *on line*, riproduzione abusiva di programmi informatici o di ogni tipo di opera intellettuale su supporto digitale (libri, musica, film), violazioni della *privacy*), l'idea del pool specializzato riprende vitalità tanto che il Procuratore Capo, cons. Manlio Minale, ed il Procuratore Aggiunto, cons. Alberto Nobili, coordinatore del dipartimento nel quale è collocato il menzionato gruppo di lavoro, nei primi mesi del 2005 lo rigenerano portando i suoi componenti a tre magistrati[3], i quali, per l'appunto, tra le altre materie che continuano a seguire, secondo le previsioni tabellari, si occupano specificamente anche di questa.

Io ed i colleghi abbiamo potuto così effettuare diverse ed interessanti indagini informatiche con risultati positivi e soddisfacenti anche in termini processuali, potendo avvalerci della valida collaborazione delle Forze di Polizia Giudiziaria esterna alla Procura della Repubblica, in particolare della Polizia Postale e della Guardia di Finanza, sia pure con le solite difficoltà derivanti dalla scarsezza di risorse umane soppiantate dallo spirito di sacrificio dei singoli collaboratori.

Successivamente, a partire dal maggio 2007, su sollecitazione dei magistrati del pool e con l'appoggio del Procuratore Aggiunto, il Procuratore Capo ha ottenuto dai Dirigenti dei rispettivi corpi di appartenenza la applicazione presso la Procura della Repubblica di una squadra di Polizia Giudiziaria specializzata in reati infornatici.

Questa soluzione organizzativa, che, peraltro, ha anticipato quella sostanzialmente introdotta dalla Legge 18 marzo 2008 n.48 relativa alla attribuzione distrettuale dei reati informatici cd. puri con corrispondente istituzionalizzazione di aliquote specializzate in questa materia presso le Sezioni di Polizia Giudiziaria di ciascuna Procura della Repubblica italiana, ha dato la possibilità di avere una visione di insieme non solo veloce ma anche più agile del panorama criminale informatico, consentendo di affinare le tecniche di accertamento e di rendere più efficaci gli strumenti di repressione così realizzando una sistema complessivamente più efficiente.

Sotto altro profilo, invero, la previsione della attribuzione alla Procura della Repubblica distrettuale dei reati cd. informatici puri stabilita dall'art. 11 Legge 18 marzo 2008 n.48, entrata in vigore il 5 aprile 2008 (norma peraltro non strettamente conforme alle previsioni della Convenzione di Budapest del 23 novembre 2001, la quale, all'art.22, intendeva far riferimento ai ben diversi problemi di giurisdizione in materia di cybercrime) ha portato un significativo impatto organizzativo quanto al numero dei procedimenti penali che si sono incardinati.

[3] Lo scrivente, il dr. Francesco Cajani e la d.ssa Elisa Francesca Moretti.

Tale previsione si è subito dimostrata priva di qualsiasi utilità sostanziale ed anzi ha creato numerosissimi problemi, non solo per il difficile raccordo normativo in relazione all'individuazione dell'Ufficio del G.I.P. territorialmente competente e per le questioni di diritto intertemporale (rispettivamente risolti dai successivi artt. 2 e 12 bis Legge 24 luglio 2008 n.125 – cd. primo pacchetto sicurezza) ma anche e soprattutto per ragioni strettamente organizzative: la maggior parte delle neonate "Procure Distrettuali Informatiche" non avevano, al momento della entrata in vigore della Legge 48/2008, magistrati già specializzati in materia di cyber crime e dediti a lavorare in pool strutturati e quindi si sono dovute organizzare ex novo.
Forse proprio prendendo spunto da questa situazione di fatto, il Consiglio Superiore della Magistratura, a livello di formazione centralizzata e decentrata, ha notevolmente implementato l'offerta formativa per i magistrati sui temi della criminalità informatica e delle nuove tecnologie, mentre a livello locale gli Uffici Distrettuali per l'Informatica hanno assunto importanti iniziative per la formazione del personale di Polizia Giudiziaria (v. corso base per gli accertamenti informatici nelle investigazioni penali destinato alla P.G. di supporto alla Procura di Milano ed a tutte le Forze dell'Ordine che collaborano con le A.G. del Distretto di Milano).
È evidente che conferire una attribuzione distrettuale a tutta la gamma, indistintamente, dei reati informatici ha significato di fatto paralizzare l'azione investigativa, dal momento che anche questioni, per così dire, bagatellari (si pensi ad una querela per un accertato malfunzionamento di una casella di posta elettronica) si aggiungono, senza una ragionevole ratio, alle notizie di reato meritevoli di sviluppo investigativo.
Sotto questo profilo, il disegno normativo avrebbe forse potuto avere una sua ragion d'essere solo ove finalizzato a migliorare le attività di contrasto di fenomeni di criminalità informatica riconducibili alle attività di gruppi organizzati e strutturati in ambito associativo.
A ciò si aggiunga che all'aumentato carico di lavoro delle "Procure Distrettuali Informatiche" non sono finora seguite – come ci si sarebbe ragionevolmente aspettato – iniziative legislative volte ad elevare il livello di conoscenza tecnica delle Forze di Polizia Giudiziaria e/o il livello di dotazioni informatiche in uso alle stesse, ancora di gran lunga obsolete per un adeguato contrasto alla criminalità, non solo informatica.

2. La cooperazione giudiziaria nelle indagini internazionali in materia di cybercrime.

Lo sviluppo delle tecnologie dell'informazione e della comunicazione (*informa-*

tion and communication techologies - ICT) e, soprattutto, delle comunicazioni via internet, ha determinato un rapidissimo cambiamento dell'organizzazione della società mondiale, modificando in profondità la struttura ed il funzionamento di fondamentali settori della vita economica e sociale.
La svolta è stata indubbiamente segnata dal progressivo sviluppo della possibilità di accesso a tali mezzi che, essendo ormai alla portata di una vasta parte della popolazione mondiale, consentono di elaborare, memorizzare e diffondere dati ed informazioni con una velocità e semplicità inimmaginabili sino a pochi anni fa.
Sono emersi, innanzitutto, nuovi rilevanti problemi d'integrazione culturale, di bilanciamento di diversi e contrastanti interessi e di disciplina giuridica di nuovi tipi di fatti e condotte non più sussumibili nelle tradizionali categorie giuridiche.
Dunque è evidente **l'inadeguatezza degli attuali sistemi giuridici nazionali ed internazionali rispetto alle sfide poste dal *cybercrime***.
Sicchè si evidenzia la **necessità di agire in plurime direzioni**[4]:

- l'armonizzazione degli ordinamenti penali degli stati nazionali sotto il profilo sostanziale e processuale;
- lo sviluppo di una politica condivisa di cooperazione giudiziaria;
- la collaborazione con gli imprenditori privati del settore;
- la messa a punto di tecniche e strumenti investigativi idonei a fronteggiare la rapidità e diffusività delle condotte dei cybercriminali.

Rispetto all'elemento di novità emerso con la diffusione del *web*, cioè la creazione di un nuovo spazio, caratterizzato da moduli spazio-temporali globalizzati, ove possono realizzarsi le più disparate condotte umane, lecite ed illecite, ed ove le stesse perdono il tradizionale rapporto di fisicità che avevano con elementi quali il luogo o il tempo entra in crisi il tradizionale concetto di sovranità degli ordinamenti e la loro pretesa di regolare autonomamente le manifestazioni umane verificatesi sul proprio territorio, potendo nel *cyberspazio* un'azione criminosa essere ideata e concordata in uno stato, eseguita attraverso delle apparecchiature site in uno o più stati differenti e produrre i propri effetti ancora in altri Stati.
A fronte di ciò, vanno sicuramente ripensati i processi di ideazione ed attuazione delle politiche criminali; così come si deve prestare la massima attenzione alla tutela di tutti gli interessi in gioco, bilanciando attentamente le esigenze di prevenzione e sicurezza e la tutela dei diritti fondamentali - tradizionali e nuovi - che oggi vengono esercitati attraverso l'accesso al *web*.

[4] È l'opinione, condivisibile, espressa dal dr. Fabio Licata, Giudice per le Indagini Preliminari presso il Tribunale di Palermo, nell'intervento "La Convenzione del Consiglio d'Europa sul cybercrime e le forme della cooperazione giudiziaria: una risposta globale alle nuove sfide della criminalità transnazionale" tenuto all'incontro di studio in Roma il 19 settembre 2005.

2.1. Le Convenzioni del Consiglio d'Europa.

2.1.1. La convenzione di Bruxelles del 29 marzo 2000 sull'assistenza giudiziaria in materia penale.

Una **cooperazione internazionale veloce ed informale** è possibile anche con riferimento alle indagini informatiche ed anzi si ritrova sia nello spirito sia nelle singole norme delle convenzioni internazionali del Consiglio d'Europa, ed in particolare nella "Convenzione stabilita dal Consiglio d'Europa conformemente all'art. 34 del Trattato sull'Unione europea, relativa all'assistenza giudiziaria in materia penale tra gli Stati membri" (Bruxelles 29 maggio 2000), che è la linea guida per il futuro, in quanto esprime una linea di tendenza che pare oramai univoca e costante, al di là di estemporanee prese di distanza di singoli Stati su singole questioni.

2.1.2. La Convenzione di Budapest del 23 novembre 2001 sul cybercrime

Il Consiglio d'Europa è stata una delle prime istituzioni internazionali ad agire sul fronte del contrasto ai crimini cibernetici, prendendo consapevolezza della necessità di superare la *"digital divide"* (la barriera digitale) tra tecnica e diritto.
Gli **obiettivi fondamentali** della Convenzione di Budapest si possono riassumere in tre punti:
1) armonizzare gli elementi fondamentali delle fattispecie di reato del diritto penale sostanziale degli ordinamenti nazionali e tutte le altre disposizioni connesse alla disciplina della *cyber criminalità* (artt. 2-13);
2) dotare le procedure penali dei paesi sottoscrittori dei poteri necessari a svolgere indagini efficaci e ad assicurare l'utile raccolta della prova penale, sia in materia di *computer crimes*, che in relazione ad ogni altro reato commesso mediante l'uso di mezzi di alta tecnologia dell'informazione e comunicazione (artt. 14-22);
3) attuare un efficace e rapido regime di cooperazione internazionale in materia, tramite lo snellimento degli strumenti di assistenza (giudiziaria e di polizia) e lo scambio di informazioni e dati in tempo reale (artt. 23-35).

2.2. La necessità dell'armonizzazione dei sistemi penali e degli indirizzi di politica criminale

Le considerazioni già svolte hanno evidenziato che **anche l'azione di contrasto deve adeguarsi e collocarsi direttamente nel nuovo mondo globale ov-**

vero deve superare i confini nazionali.
I punti nodali dello sviluppo di tale processo sono i seguenti:
1. la scelta di modelli d'incriminazione penale minima che consentano un'adeguata integrazione fra gli ordinamenti nel rispetto delle garanzie sostanziali e processuali e delle peculiarità culturali e giuridiche di ciascuno stato;
2. un adeguato sistema di rapporti bilanciati tra organismi nazionali e sovranazionali, finalizzato ad un'efficace individuazione dei principi della produzione normativa;
3. l'individuazione, nel rispetto delle specificità culturali, del livello della tutela penale da apprestare ai nuovi beni da proteggere;
4. la necessità di non imbrigliare in regole eccessivamente rigide un mondo come quello della rete, caratterizzato proprio dal massimo livello di libertà di circolazione delle idee e informazioni.
Il raggiungimento di questi obiettivi di armonizzazione globale degli ordinamenti penali, peraltro, non è solo la condizione necessaria per ottimizzare il contrasto alle nuove forme di criminalità cibernetica, ma anche lo strumento per evitare che vi siano paesi individuabili come "paradisi del cybercrime", sul modello di quelli già preferiti dai criminali come basi per il riciclaggio di denaro sporco grazie alle garanzie assicurate dalle legislazioni nazionali.

2.3. La cooperazione giudiziaria nelle indagini internazionali in materia di cybercrime.

La reciproca assistenza giudiziaria è cruciale nello svolgimento di indagini internazionali in materia di cybercrime, tenuto conto che lo sviluppo veloce, le reti e l'aumento delle velocità di collegamento consentono ai criminali di eludere molto più rapidamente e facilmente le tecniche investigative tradizionali. Nei casi del cybercrime una delle caratteristiche fondamentali della prova digitale è la velocità con cui viaggia e la volatilità dei dati che, facilmente, sono cancellati, alterati, copiati, conservati, trasferiti e distrutti. Il tracciamento di un percorso elettronico, finalizzato all'identificazione di un sospetto, ha come esigenza primaria la conservazione dei dati e, sotto il profilo giuridico, tali dati devono essere conservati e raccolti in modo da conservare la loro integrità probatoria secondo le regole e le garanzie del processo penale.
Dunque, **i fattori fondamentali per il successo di un'indagine sul *cybercrime* a dimensione internazionale** sono quello della velocità degli atti investigativi e della raccolta dei dati secondo le regole dell'ordinamento penale nazionale ove le prove debbono essere fatte valere.
Nella consapevolezza di tali presupposti, la convenzione sul Cybercrime, nel porre i principi generali della materia, si ispira al massimo favore per la coope-

razione internazionale, stabilendo all'art. 23 che "le parti devono cooperare tra loro nella misura più ampia possibile nelle indagini o nei procedimenti riguardanti reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma elettronica, di un reato, in conformità alle disposizioni di questo capitolo e in applicazione degli strumenti internazionali sulla cooperazione in materia penale, degli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e del loro diritto nazionale".
Sono **tre i principi generali** ricavabili da tale disposizione:
1) le parti devono cooperare le une con le altre nella misura più larga possibile;
2) la cooperazione deve estendersi a tutte le infrazioni penali legate a sistemi o dati informatici, così come alla raccolta di prove in forma elettronica;
3) la cooperazione deve tenere in conto l'applicazione degli strumenti internazionali pertinenti, relativi proprio alla cooperazione in materia penale, o degli accordi fondati su delle legislazioni uniformi o reciproche nel diritto nazionale degli Stati che entrano in contatto tra loro.
In attesa e nella prospettiva di realizzare una cooperazione internazionale effettivamente corrispondente agli impegni assunti nei trattati internazionali menzionati sembra imprescindibile un approccio pragmatico che, pur nel continuo mutare delle regole interne dei vari Stati delle regole convenzionali, si fondi su alcuni punti fermi corrispondenti a quelle linee di pensiero sostanzialmente consolidate e condivise, espresse esplicitamente nella disciplina menzionata e che sono:
1) il rapporto diretto tra autorità giudiziarie, non mediato né rallentato da autorità politiche;
2) la velocità della cooperazione, che in fase di indagini deve adeguarsi alla velocità dei criminali (basti pensare ad una consegna controllata transnazionale: o si segue il carico in tempo reale, oppure non se ne fa nulla);
3) l'assenza (quasi totale) di formalità.
Invero un'efficace azione di contrasto al cybercrime non può prescindere dalla cooperazione dinamica tra le magistrature e tra le forze di Polizia e tra le prime e le seconde che deve partire già dal momento iniziale delle indagini in tema di reati informatici,
Mi riferisco non all'attività rogatoriale classica, alla tradizionale richiesta di prove e/o di svolgimento di attività investigativa, bensì al quotidiano, velocissimo, frenetico scambio di dati e notizie tra Autorità Giudiziarie e tra Polizie Giudiziarie di Stati diversi nel corso delle indagini.
La **cooperazione dinamica** si propone di svolgere insieme le indagini mentre i fatti avvengono, al fine di poter ragionevolmente arrivare ad un risultato investigativo completo, con la ricostruzione precisa e dettagliata dei fatti-reato og-

getto delle indagini e con l'accertamento delle eventuali responsabilità penali di tutti i protagonisti del crimine perseguito; risultato investigativo ben difficile da realizzare altrimenti e che sarebbe destinato a fermarsi con una richiesta di archiviazione per essere gli autori dei fatti rimasti ignoti in quanto non identificabili all'estero, ovvero, nella migliore delle ipotesi, che si limiterebbe all'identificazione ed alla celebrazione del processo nei confronti dei soli soggetti che agiscono all'interno del proprio Stato, lasciando che gli altri, operando in altro Stato, si sentano indisturbati e, quel che è peggio, impuniti.
Un'effettiva ed efficace cooperazione internazionale porta almeno i seguenti due risultati rilevantissimi:
1) in primo luogo, consente di comprendere a fondo fenomeni dei quali, altrimenti, quasi neppure si sospetterebbe l'esistenza, e di raccogliere prove sull'intera catena criminale e non solo sul singolo anello che ha agito in Italia (si pensi al *phishing,* alle frodi o ai sabotaggi di sistemi su larga scala, all'utilizzazione abusiva sistematica di carte di credito, alle cd. *cyber-estorsioni*, al riciclaggio del denaro sporco attraverso i casino virtuali, le aste on-line, l'*online banking* o la compravendita di titoli vari mediante transazioni elettroniche rapide ed anonime, alla pedopornografia on-line, alla prostituzione on-line, alle truffe commerciali online, alla contraffazione di beni realizzati e venduti tramite il computer, alle molestie informatiche (il c.d. *cyberstalking*), al gioco d'azzardo online, alla riproduzione abusiva di programmi informatici o di ogni tipo di opera intellettuale su supporto digitale (libri, musica, film), all'accesso illecito a banche di dati personali o alla raccolta e la diffusione abusiva di tali dati (prelevati dai *personal computers* a mezzo dei *cookies* o di altro *spyware)*, all'incitamento, all'istigazione o alla trasmissione di istruzioni relative alla realizzazione dei più svariati crimini o al proselitismo terroristico, ecc.);
2) in secondo luogo, l'azione repressiva ha una maggiore efficacia, in quanto gli Stati interessati, che vengono messi al corrente delle indagini condotte in uno Stato, agiscono direttamente nei confronti dei reati commessi nel loro territorio. Quest'ultimo è un profilo da non sottovalutare, e che va al di là della normale collaborazione internazionale: più che far condannare in contumacia i criminali che vivono ed operano all'estero, e che mai verranno estradati dai loro Paesi, talora può forse essere preferibile farli condannare dai loro stessi Paesi; il risultato consiste in un'effettiva punizione ed un effettivo contrasto della criminalità informatica transnazionale.
Ma come si concretizza questo tipo di cooperazione dinamica? Come si arriva ad una cooperazione così intensa, penetrante, totale?
Innanzitutto occorre **fiducia reciproca** altrimenti la normativa internazionale in materia resterebbe inapplicata ed anzi inapplicabile.
Il che comporta che vanno intensificati i rapporti diretti, segnalando ai colleghi

e/o alle forze di Polizia appartenenti allo Stato interessato dalle indagini, previamente individuati attraverso gli organismi europei di coordinamento menzionati, per esempio i luoghi in cui sono allocati i *server* che interessano, richiedendo loro i dati del traffico telefonico e/o telematico utili allo sviluppo delle indagini, indicando le utenze telefoniche che è stato accertato essere in uso agli indagati o comunque essere indispensabili alle indagini, mediante attività inizialmente priva di formalismi; così che sulla base di tali segnalazioni i corrispondenti colleghi disporranno perquisizioni, ispezioni e sequestri informatici presso le società ove sono allocati i *server,* provvedimenti per l'acquisizione di dati del traffico telefonico e/o telematico presso i *provider,* intercettazioni, pedinamenti e quant'altro, con il rilevantissimo risultato che da quel momento in avanti tutti gli investigatori saranno a conoscenza nei dettagli delle indagini e saranno in grado di ricostruire fedelmente il fatto che ne occupa e di risalire alle eventuali responsabilità con certezza.

Non solo ma, a mio avviso, sarà essenziale istituzionalizzare gruppi di magistrati e forze di Polizia specializzati sulla criminalità informatica (sulla falsariga del pool della Procura della Repubblica milanese e di qualche altra Procura della Repubblica italiana), i quali, sollecitati dagli organismi europei di coordinamento e di intelligence (Eurojust, Olaf, e quant'altro) che la Procura inquirente avrà tempestivamente avvisato, si attivino efficacemente in tempo reale ad ogni richiesta di cooperazione proveniente da altro Stato europeo.

In conclusione la cooperazione giudiziaria informale, che è assimilabile e/o sovrapponibile alla collaborazione tra le forze di polizia, è veloce, dinamica e consente di rispettare le esigenze delle indagini informatiche.

Naturalmente i risultati investigativi vanno acquisiti formalmente con le forme rogatoriali previste dalle leggi vigenti ai fini della loro utilizzabilità in giudizio.

Finito di stampare nel mese di gennaio 2011
presso L.E.G.O. spa, Lavis (TN)

A partire dal 2008 l'annuale Convegno di studi, promosso sin dal 2001 con la collaborazione dell'Ufficio Europeo per la lotta antifrode (OLAF) e dell'Unione degli Avvocati Europei (UAE), dapprima a Como poi a Milano, si è arricchito sempre più di contributi scientifici - di volta in volta in linea con le tematiche trattate - attinenti la variegata (e quanto mai, in Italia, poco conosciuta) materia della computer forensics. Proprio in quanto destinate ad un siffatto contesto, le problematiche ivi affrontate dai relatori (sia italiani che stranieri) individuati dall'Associazione IISFA (International Information Systems Forensic Association) hanno costituito una importante occasione per una analisi non già fine a se stessa, ma idonea ad indicare una prima prospettiva europea attinente al più generale settore degli accertamenti informatici nelle investigazioni penali. Si ripropone il frutto di tale analisi con la pubblicazione di alcuni tra gli interventi più significativi, corredati da altri materiali ricollegabili alla attività scientifica di IISFA in contesti europei negli ultimi tre anni.

AUTORI DEI CONTENUTI

Stefano Aterno - *Avvocato in Roma, Vicepresidente IISFA Italian Chapter*
Francesco Cajani - *Sostituto Procuratore della Repubblica presso il Tribunale Ordinario di Milano - pool reati informatici*
Massimiliano Carducci - *Sostituto Procuratore della Repubblica presso il Tribunale Ordinario di Milano - pool reati informatici*
Gaia Cingolani - *Secretary IISFA Italian Chapter*
Gerardo Costabile - *CIFI, CHFI, ACE, CGEIT - Presidente IISFA Italian Chapter (www.iisfa.net)*
Davide Gabrini - *Computer Forensics Expert ed investigatore della Polizia Postale e delle Comunicazioni di Milano*
Giorgio Lattanzi - *Presidente di Sezione della Corte di Cassazione*
Luca Luparia - *Docente di Diritto Processuale Penale presso l'Università di Teramo*
Stephen Mason - *Barrister and member of the IT Panel of the General Council of the Bar of England and Wales*
Alexander Seger - *Council of Europe, Economic Crime Division - Directorate General of Human Rights and Legal Affairs*
Frédéric Van Leeuw - *Federal Magistrate at the Federal Prosecutor's Office of Belgium, Reference magistrate in matters of cybercrime - Section Organised Crime*
Giovanni Ziccardi - *docente di Informatica Giuridica Avanzata presso l'Università di Milano*