LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di GIURISPRUDENZA

Cattedra di INFORMATICA GIURIDICA

L'UTILITÀ DELLA COMPUTER-FORENSICS NEL PROCESSO PENALE: NUOVE TECNOLOGIE E PRASSI

RELATORE

Prof. Gianluigi Ciacci

CANDIDATO

Antonio Sapio

Matr. 112833

CORRELATORE

Prof.ssa Barbara Sargenti

ANNO ACCADEMICO 2015/2016

Alla Sig.ra Antonietta

INDICE

INTRODUZIONE

Lo scopo di questo elaborato è di analizzare nello specifico le norme, le dinamiche e le applicazioni pratiche della computer forensics, la scienza in ambito giuridico che ruota attorno le diverse operazioni da compiere sul dato informatico ai fini di una valutazione come prova all'interno di un processo. Nel tal caso particolarmente del rito penale, con l'intento di comprendere quanto oggi essa sia necessaria ed incisiva all'interno di un ordinamento giuridico. In primo luogo osserveremo come oggi le prassi e le principali linee guida siano inserite all'interno del sistema italiano; poi citeremo le recenti modifiche nel codice di procedura penale, indicando anche le principali istituzioni italiane che si avvalgono di queste procedure nelle loro mansioni. Successivamente si approfondiranno le diverse fasi della computer forensics, iniziando dalle indagini fino ad arrivare al sequestro, alla certificazione e all'acquisizione in tribunale da parte dei giudici, soffermandoci anche sui principali dispositivi oggetto di esame, nonché le tecniche e gli strumenti più adottati nella prassi dagli inquirenti, con particolare attenzione ai più recenti. Di seguito verrà illustrato un "*case study*" sulle vicende dell'omicidio Garlasco ad opera di Alberto Stasi, ritenutosi questi un prezioso esempio riguardo la rilevanza ad utilizzare procedure standardizzate quando si rinviene del materiale informatico su una scena del crimine. Al termine effettueremo una panoramica delle principali innovazioni in campo tecnologico-investigativo che potrebbero essere introdotte in Italia in un prossimo futuro, cui seguirà una comparazione delle esperienze di computer forensics più significative negli ordinamenti sia delle nazioni che recentemente si stanno approcciando a questa disciplina, così come di quelle che ormai la praticano da tempo. Nelle conclusioni verrà rassegnato un resoconto del nostro studio.

CAPITOLO 1

Introduzione alla computer forensics

1.1 *Cosa è la computer-informatic forensics ?*

L'evoluzione della tecnologia ha prodotto e sta producendo considerevoli cambiamenti nel modo di condurre le nostre vite, nelle interazioni sociali e negli approcci della persona nei confronti della realtà. In tutto ciò non poteva non esserne coinvolto il Diritto, essendo quest'ultimo un fenomeno strettamente collegato all'essere umano, alla società e alle relazioni tra quest'ultimi. Su questa linea anche il Diritto si è evoluto, cercando di comprendere e disciplinare le nuove contingenze e risolvere i problemi legati all'utilizzo di sistemi informatici e computerizzati, essendo quest'ultimi non più limitati a una ristretta cerchia di persone per questioni lavorative o di passione, ma essendo, invece, ormai estesi a qualsiasi età o classe sociale[1]. Bisogna considerare, inoltre, l'altra faccia della medaglia: la tecnologia non è solo oggetto di studio del giurista, per comprendere come essa influenzi i concetti delle normative, ma è anche uno strumento per agevolarne i compiti e per ottenere migliori risultati. Soprattutto nel campo investigativo poi l'apporto migliorativo dato dalle nuove tecnologie, che nell'ultimo mezzo secolo ha fatto passi da gigante, è stato notevole, facendo sì che si creassero nuove prassi e metodologie funzionali ad affrontare sia i crimini che sono nati attraverso un distorto utilizzo dei nuovi mezzi informatici- telematici creando nuove fattispecie, sia i crimini che potremmo definire "*storici*", compiuti oggi spesso e volentieri mediante strumenti tecnologici di nuova generazione[2] (basti pensare ad esempio al reato di diffamazione che oggi può essere anche comune su blog pubblici o sui giornali on-line, oppure a reati ancor più gravi

[1] M. Solomon, D. Barrett, N. Broom, *Computer Forensic Jumpstart*, Sibex, 2004.
[2] G. Costabile*, Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Ciberspazio e diritto*, 3, 2010, pag. 465.

come l'estorsione o la truffa posti in essere attraverso uno smartphone o da un pc). Tale evoluzione ha reso necessaria la creazione di sezioni specializzate nei corpi di polizia che fossero istruite e competenti nell'effettuare indagini per i reati informatici. Nasce così anche l'informatica forense, meglio conosciuta col termine anglosassone di computer-informatic forensics. Quest'ultima viene definita come «*la scienza che studia sia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione, e ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico, sia le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici ai fini probatori*»[3]. Ciò premesso possiamo constatare che la computer-forensics può essere suddivisa ed esaminata essenzialmente su due piani:

a) il primo è quello legato strettamente al dato informatico (o anche detto "*file*"), ossia «*qualsiasi rappresentazione di fatti, informazioni o concetti idonei ad essere oggetto di trattamento ed elaborazione da parte di un programma o un sistema informatico*»[4];

b) il secondo è invece di natura più pratica ed abbraccia l'aspetto tecnico della materia, occupandosi di studiare e poi in seguito statuire come deve muoversi in questo campo l'investigatore-forenser senza correre il rischio di inquinare la scena del crimine oppure tralasciare e/o danneggiare materiale probatorio informatico di una certa rilevanza, tenendo conto inoltre di quali tra le prove reperite, sarebbero ammissibili in un processo penale all'interno dell'ordinamento italiano[5].

Bisogna specificare che oggi giorno sono diffuse ormai vere e proprie linee guida (c.d. "*Best Practice*"), che disciplinano ed espongono i passi che devono essere fatti per l'acquisizione in maniera corretta del dato informatico per essere valutato in maniera idonea all'interno di un processo. Sebbene l'efficacia e la condivisione delle best practice sia oggi accertata a livello internazionale, in Italia non sono vincolanti, essendo queste buone pratiche paragonabili, sul piano dell'obbligatorietà nell'essere osservate, a quelle utilizzate in campo medico sulla responsabilità professionale del sanitario. Tuttavia sia attraverso le influenze da

[3] G. Amato, V. Destito, G. Dezzani, C. Santoriello*, I reati informatici. Nuova disciplina e tecniche processuali di accertamento*, Roma, Cedam, 2010, pag. 173 e ss.
[4] G. Amato, V. Destito, G. Dezzani, C. Santoriello, *Op. Cit.*, pag. 4 e ss.
[5] A. Ghirardini, G. Faggioli, *Computer Forensics*, Apogeo, 2009.

parte delle legislazioni del Regno Unito e statunitensi, sia grazie alla Convenzione di Budapest del 23 Novembre 2001, il nostro ordinamento, solo con la legge di ratifica[6] della Convenzione sopracitata, con le relative modifiche ed integrazioni al codice penale e al codice di procedura penale, si è portato agli standard minimi necessari per poter garantire un' adeguata lotta non solo al "*Cybercrime*", ma anche a favorire oggi un maggior rigore nell'acquisizione delle prove informatiche nell'ambito processuale e nella sicurezza dei sistemi informatici più in generale al pari delle altre nazioni all'avanguardia in questo settore[7]. Lo studio delle tecniche informatiche per effettuare indagini sempre più accurate ed efficaci è sicuramente l'aspetto più interessante della materia, poiché si tratta di pura innovazione sia tecnologica che giurisprudenziale. Si è infatti già detto che questa è la parte più pratica della computer forensics e non meraviglia che sia strettamente collegata a quella parte del diritto volta appunto a risolvere i problemi concretamente, ossia le sentenze dei giudici. Quest'ultime, decisione dopo decisione, hanno fatto da apripista a molti metodi e sistemi rivoluzionari che hanno portato a una graduale integrazione delle indagini informatiche nel nostro ordinamento, andando a colmare quelle lacune o zone grigie che potevano esser stati lasciati dalle normative.[8]

1.2 *L'utilità della computer-informatic forensic nella procedura penale e come contribuisce all'interno del sistema italiano*

Come anticipato, la legge di ratifica della convenzione di Budapest (legge n. 48 del 2008) ha portato significative novità all'interno del codice di procedure penale, andando ad inserire diversi e nuovi elementi nell'ambito delle perquisizioni e delle ispezioni, e facendo fronte alla necessità di adeguamento delle Procure ai protocolli internazionali in merito a questo tipo particolare di

[6] Legge n. 48 del 18 marzo 2008, "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*".

[7] D. Littlejohn Shinder, E. Tittel, *Scene of the Cybercrime. Computer Forensics Handbook*, Syngress, 2003.

[8] M.L. Di Bitonto, *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. dell'internet* , 2008, Ipsoa.

indagini[9]. Tuttavia nonostante il grosso passo in avanti il legislatore si è mostrato piuttosto cauto nell'adattare la disciplina, adottando (probabilmente volutamente) definizioni late e generiche e soffermandosi più sul risultato finale da perseguire che sulle metodologie da usare[10], scelta per certi versi condivisibile da un punto di vista pratico e applicativo, ma che ha lasciato diverse perplessità interpretative colmate dalla giurisprudenza. In particolar modo la legge di ratifica e andata ad introdurre e/o modificare una serie di reati nel codice penale. Tra i più importanti: il falso informatico (art. 491 bis c.p.), la falsa dichiarazione o attestazione al certificatore di firma elettronica (art. 495 bis c.p.), la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.), il danneggiamento informatico (art. 635 bis, art. 635 ter, 635 quater, 635 quinquies c.p.) e la frode del soggetto che presta servizio di certificazione di firma elettronica (art. 640 quinquies c.p.)[11].

Le modifiche al codice di procedura penale, invece, sono state effettuate quasi in maniera chirurgica, facendo si che si innestassero al meglio nel tessuto normativo senza creare troppi sconvolgimenti o dubbi agli organi inquirenti. L'obiettivo del Legislatore in questo caso, è stato quello di aggiornare la disposizione introducendo i principi cardine della computer forensics ossia la necessità di tecniche che assicurino la conservazione dei dati originali e l'adozione di procedure che non alterino i dati stessi[12]. Il primo intervento lo ritroviamo nell'art. 244 comma 2, secondo periodo del c.p.p., dove troviamo inserite le parole: «*anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*».

Il secondo articolo modificato è stato l'art. 247 c.p.p. (in materia di perquisizioni) con un nuovo comma 1-bis che recita: «*quando vi è fondato motivo*

[9] G. Costabile*, Op. cit*., pag. 469 e ss.
[10] G. Ziccardi, *L'ingresso della computer forensic nel sistema processualpenalistico italiano: alcune considerazioni informatic- giuridiche*, in L. Luparia, *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*, Giuffré, 2009, pag. 165.
[11] G. Amato, V. Destito, G. Dezzani, C. Santoriello, *Op. cit*.
[12] G. Ziccardi, *Op. cit.,* pag.167.

di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Si può notare come viene rafforzato il potere inquisitorio degli organi investigativi, in maniera tale da consentirgli una più efficace e produttiva raccolta di informazioni senza incorrere blocchi di natura tecnica che ne impedirebbero una corretta acquisizione. Stesso concetto viene ripreso nella modifica sull'art. 248 comma 2 c.p.p. dove si stabilisce che « *per rintracciare le cose da sottoporre a sequestro o per accertare altre circostanze utili ai fini delle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria da questa delegati possono esaminare presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici. In caso di rifiuto, l'autorità giudiziaria procede a perquisizione*».

La terza modifica investe l'art. 254 del c.p.p. (sul sequestro di corrispondenza) che ha aggiunto l'art. 254-bis: «*L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali*». In questo caso il legislatore è andato ad operare una decisione di compromesso in quella che è un'annosa diatriba nella dottrina della computer forensics (meglio sequestrare l'intero supporto fisico corpo del reato o oggetto pertinente al reato, oppure eseguire delle copie certificate ?). È chiaro che non vi può essere una decisione definitiva, ma valutata la situazione volta per volta in base al caso concreto, cosicché con questa disposizione attraverso l'utilizzo delle parole "*può stabilire*" lascia discrezionalità agli investigatori su come agire.

La quarta modifica interessa l'art. 256 c.p.p. (dovere di esibizione e segreti) con l'inserimento della frase: «*nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto*», quindi una

semplice estensione all'ambito informatico della precedente normativa. Un'ulteriore modifica ha coinvolto anche il campo dei sequestri concentrandosi soprattutto sulla genuina tenuta e conservazione del materiale informatico, che a differenza degli altri reperti probatori necessità di particolari condizioni di custodia. Nello specifico ora la norma prevede che «*quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria*». Si focalizza ancora l'attenzione sulla «corretta procedura di realizzazione della copia, la sua conformità all'originale e la sua immodificabilità[13]». Continuando sulle perquisizioni, quest'ultime vengono ancora toccate da un ulteriore articolo (art. 352 c.p.p.) con un comma bis che specifica che «*nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi*». Anche qui si riprendono altri principi della computer-digital forensics nonché concetti espressi negli articoli prima espressi, ma con l'attenzione di farli ricadere anche in quei casi di particolare urgenza dove la celerità può essere significativa (come appunto la flagranza di reato).

Infine, il nostro esame della legge di ratifica e delle sue innovazioni si conclude con l'art. 354 comma 2 c.p.p. (accertamenti urgenti sulle cose e sulle persone), dove troviamo inserito un nuovo periodo: «*In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottando, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata*

[13] G. Ziccardi, *Op. cit*., pag. 169.

duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità». Anche questa norma non aggiunge nulla di veramente rilevante che non venga già esposto dalle precedenti integrazioni, ma mostra quale sia la ratio legis della Convenzione di Budapest e riserva una particolare attenzione alla ricerca della prova, sulla maggior sicurezza e attenzione nel reperimento e sulla custodia.

1.3 *Il contributo della Computer-informatic forensics in altri campi nazionali*

Le novità apportate dalla legge n. 48 del 2008 non soltanto hanno influenzato il modo di agire e di pensare dei giuristi, dovendo quest'ultimi aggiornare le loro conoscenze sia che fossero giudici o avvocati per necessità della loro professione, ma data la peculiarità del settore coinvolto della procedura penale, ovvero il libro III delle prove, hanno portato sconvolgimenti ed evoluzioni anche in altri ambiti lavorativi che, sebbene affini o collegati, esulano dalle aule di tribunale. Primi pionieri di questo settore sono stati sicuramente gli ingegneri informatici. Ancora oggi quest'ultimi svolgono un ruolo cardine nel sistema italiano essendo i maggior conoscitori dell'ambito informatico e sapendo quindi come muoversi e destreggiarsi all'interno di esso. Non a caso, quando ancora il fenomeno del "*Cybercrime*" non era elevatamente diffuso e la tecnologia di un certo livello era solo un vezzo per pochi, si ricorreva sempre alla perizia o al parere tecnico dell'ingegnere informatico. Tuttavia ben presto questo sistema cominciò a sentire delle pecche, per il semplice fatto che, con l'evoluzione tecnologica descritta nei primi paragrafi e l'immanenza della tecnologia nella vita di tutti i giorni, cominciava a divenire prassi il ricorrere ad un tecnico specializzato. Sicché si è cominciato a capire che sarebbe stato molto più semplice istruire e aggiornare gli operatori del diritto nonché creare fin dagli studi universitari corsi di specializzazione appositi. In questo modo non si potevano neanche più creare incomprensioni o malintesi tra chi scriveva la perizia e chi la andava a leggere essendo ormai quest'ultimo abbastanza edotto sulla materia (tanto è vero che ormai si ricorre agli ingegneri informatici soltanto per casi di elevata complessità dove è necessaria una vera propria competenza specifica).

Tirando le somme se da una parte giudici ed avvocati sono diventati più pratici nella materia informatica, potendo fare a meno per i casi ordinari di uno specialista, tuttavia ancora in alcuni casi di particolare gravità è necessaria la presenza di un esperto, sebbene appunto il loro ausilio è stato drasticamente ridotto e più che altro reindirizzato verso settori di ricerca nelle tecniche investigative.

Nel processo di rinnovazione non potevano non essere coinvolti anche i vari rami delle forze dell'ordine e della polizia giudiziaria. Infatti attraverso la legge riforma dell'Amministrazione della Pubblica Sicurezza viene istituita la "*Polizia Postale e delle Comunicazioni*", un reparto specializzato della Polizia di Stato «*all'avanguardia nell'azione di prevenzione e contrasto della criminalità informatica e a garanzia dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione. Il principale sforzo operativo della "Polizia Postale e delle Comunicazioni" è nella direzione del continuo adeguamento della propria risposta alle nuove frontiere tecnologiche della delinquenza*»[14]. La nascita di una forza di polizia così specializzata non meraviglia più di tanto se si tiene sempre a mente di come oggi giorno siano necessarie determinate competenze tecniche, soprattutto nell'ambito investigativo o di lotta al crimine dove il più piccolo errore può creare la più grande ingiustizia. Presso la Polizia Postale e delle Comunicazioni è stata istituita un'apposita unità di analisi del crimine informatico (Computer Crime Analysis Unit) detta anche U.A.C.I.. Quest'ultima si occupa di affiancare gli investigatori della polizia postale e delle comunicazioni nelle indagini sui crimini ad alta tecnologia, progettando nuove tecniche investigative e tracciando profili psicologici e comportamentali degli autori di tali crimini. L'unità è composta principalmente da investigatori e tecnici esperti del settore.

Le loro principali funzioni riguardano:

1) ricerche e studi sul fenomeno della criminalità informatica in collaborazione con Università, Aziende ed Istituzioni;

[14] www.commissariatodips.it/profilo/presentazione.html

2) sperimentazione di nuove tecniche investigative in materia di computer crime;
3) progettazione di percorsi di formazione sulla sicurezza informatica e computer crime in collaborazione con Università e aziende;
4) divulgazione di informazioni e risultati di ricerche in contesti scientifici;
5) assistenza psicologica degli investigatori che si occupano di computer crime (soprattutto per i reati di pedofili).

Dalle principali attività si evince subito che il lavoro svolto dall'U.A.C.I. è per lo più di supporto sia che riguardi la ricerca o l'informazione sia che invece interessi qualcosa di più pratico come le indagini. Ruolo da non sottovalutare ed anzi di massima importanza tenendo conto della velocità con cui avanza il progresso tecnologico. Da qui è chiaro che si rende necessaria anche la collaborazione con veri e propri istituti di ricerca, quali laboratori ed università, in maniera tale da essere a stretto contatto con quelle che possono essere nuove scoperte, informazioni o innovazioni da parte dei ricercatori, ed acquisirle nel proprio bagaglio di competenze sul campo. Questo approccio si sta sicuramente rivelando produttivo ed efficace se si pensa che anche altri istituti di investigazione come l' I.S.T.I dei Carabinieri di Velletri ed anche altre divisioni R.I.S. stanno seguendo l'esempio della Polizia postale e delle comunicazioni, dotandosi di apposite strutture e mezzi o comunque appoggiandosi a laboratori universitari per svolgere le proprie indagini. La necessità di un corpo con siffatte competenze fa si che oggi la polizia postale e delle comunicazioni sia presente su tutto il territorio italiano in 20 compartimenti, con competenza regionale, e 80 sezioni con competenza provinciale, coordinati a livello centrale dal Servizio Polizia delle Comunicazioni. Gli uffici sono dotati di indirizzi e-mail ai quali è possibile chiedere informazioni o inviare segnalazioni di violazione di norme penali nei vari settori di cui si occupano.

Infine meritano menzione anche gli istituti denominati A.I.S.E. (L'Agenzia informazioni e sicurezza esterna) e A.I.S.I. (L'Agenzia informazioni e sicurezza interna) che per le materie di cui trattano entrambi non potevano anche loro non esimersi dagli aggiornamenti tecnologici e dalle nuove tecniche investigative informatiche. L' A.I.S.E. *«ha il compito di ricercare ed elaborare tutte le informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza*

della Repubblica dalle minacce provenienti dall'estero. In particolare sono di sua competenza:

a) le attività di informazione per la sicurezza che si svolgono al di fuori del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia;

b) l'individuazione e il contrasto al di fuori del territorio nazionale delle attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali;

c) le attività di contro proliferazione di materiali strategici»[15].

Al pari l'A.I.S.I. si occupa di elaborare e ricercare le informazioni che invece potrebbero essere «*utili a difendere la sicurezza interna della Repubblica e le istituzioni democratiche da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica. Le sue principali attività sono*:

a) le attività di informazione per la sicurezza che si svolgono all'interno del territorio italiano, a protezione degli interessi politici, militari, economici scientifici e industriali dell'Italia;

b) l'individuazione e il contrasto all'interno del territorio italiano sia delle attività di spionaggio dirette contro l'Italia sia di quelle volte a danneggiare interessi nazionali»[16].

Merita un maggior approfondimento la prima organizzazione citata, poiché nasce da quella corrente internazionale, favorita soprattutto dall'unione europea anche attraverso l'europol, di creare un fronte coeso contro le minacce esterne, in particolar modo quelle con fini eversivi o terroristici. E' scontato ormai oggigiorno che gruppi criminali e terroristi si servano sempre più di particolari azioni criminogene legate all'informatica, come "*l'hacking"* e il "*cracking*" (con il primo termine si intendono le operazioni per accedere e modificare un sistema hardware o software, mentre col secondo le tecniche e le operazioni per violare sistemi informatici collegati ad Internet o ad un'altra rete, allo scopo di

[15] www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aise.html
[16] www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aisi.html

danneggiarli, di rubare informazioni oppure di sfruttare i servizi telematici della vittima), per realizzare passo dopo passo piani criminosi ben articolati e complessi che possono colpire la società su diversi fronti. Spesso infatti la più grande paura degli stati moderni è quella di subire una "*Cyberwar*" (diversi attacchi informatici che avvengono nel cyberspazio)[17] che disabiliti dai sistemi informatici di credito-finanziario, fino a quelli di sicurezza interna dei ministeri di difesa e via discorrendo. Ciò porterebbe l'essere umano indietro di più di una cinquantina di anni, creando quindi un grosso vantaggio tattico per le associazioni a delinquere o le cellule terroristiche. A fronte di questo grande timore si spiega quindi come i governi abbiamo impiegato risorse e strutture per tutelarsi da eventuali attacchi informatici su larga scala, concentrandosi anche in particolar modo sulla sicurezza preventiva aggiornando i propri mezzi informatici e telematici e affinando tecniche investigative adeguate per affrontare, prevenire e debellare le diverse minacce. Il diritto italiano è pressoché scarno di misure volte a contrastare questo fenomeno. Questo perché nel nostro Paese «*esiste una pluralità di organismi, poco coordinata fra di loro. Ciò rende più importante che i Servizi si interessino al settore e svolgano un ruolo trainante sia nella strategia di riduzione della vulnerabilità (aumento della resilienza sistemica), sia in quella di risposta, a partire dall'alteramento fino a giungere alla valutazione dei danni. Beninteso, anche in questo settore, i Servizi non possono fare tutto da soli*»[18]. In Italia principalmente è investito di questo compito il Dipartimento delle informazioni per la sicurezza (D.I.S), tra i cui membri vi è anche il Presidente del Consiglio dei ministri, che appunto coordina e assicura la funzionalità dell'attività dell' A.I.S.E. e dell'A.I.S.I., ruolo maggiormente potenziato con la legge 133/2012[19], per il rafforzamento delle operazioni strategiche e di sicurezza. Inoltre «*la stessa legge assegna al D.I.S. il coordinamento delle attività informative indirizzate alla protezione delle infrastrutture critiche e dello spazio cibernetico del Paese, un settore nel quale il Governo è attivamente impegnato sia sul versante della*

[17] P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital crime and Forensic science in Cyberspace*, Idea Group Publishing, 2006.
[18] C. Jean, P. Savona, *Intelligence Economica*. *Il ciclo dell'informazione nell'era della globalizzazione*, Rubettino, 2011, pag. 65.
[19] Legge n. 133 del 7 agosto 2012, "*Modifiche alla legge 3 agosto 2007", n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto "*.

prevenzione sia su quello della gestione di eventuali atti ostili»[20]. Per dovere di completezza è inoltre utile aggiungere che il Dipartimento, dopo la legge 124/2007[21], si occupa anche di promuovere l'istruzione e la formazione, attraverso una scuola specialistica, nei campi sopra definiti, allo scopo di creare un personale competente e professionalizzato da impiegare in vari settori di intelligence, sicurezza e cybercrime.

[20] https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html
[21] Legge n.124 del 3 agosto 2007, "*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*".

CAPITOLO 2

La computer forensics nelle sue diverse fasi: dal reperimento della prova fino alla certificazione della sua validità

2.1 *Campo probatorio: Ricerca fonti di prova (tipiche e atipiche)*

Quando ci occupiamo di "*cybercrime*" e più in generale di reati dove sono coinvolti sistemi informatici, vuoi perché sono il mezzo con cui è stato compiuto il reato vuoi perché sono semplici fonti di prova, ci troviamo inevitabilmente in un ambiente particolare[22]. Questo perché, al contrario delle investigazioni canoniche, il computer-forenser svolge le sue operazioni non in un mondo fisico, quindi soggetto alle leggi naturali, ma in uno telematico-virtuale dove determinate procedure possono avere esiti diversi dal mondo fisico al quale siamo abituati. Quindi, essendo il risultato delle operazioni per nulla scontati, si giustifica una particolare accortezza e attenzione a quello che il lavoro dell'inquirente, nonché delle eccezioni a quelle che sono le prassi investigative. Solitamente l'approccio che si compie nell'individuare delle prove è quello di sfruttare le abilità sensoriali umane in maniera tale da classificare ed analizzare ciò che si ha davanti. Purtroppo con i file e i byte (principali componenti delle prove informatiche) non si può fare lo stesso, poiché se fossimo rigorosamente analitici e concreti nell'esaminarli, da un punto di vista realistico arriveremmo alla conclusione che ci troviamo soltanto davanti ad un insieme di combinazioni numeriche binarie composte da zero e uno[23]. Ciò detto chi oggigiorno compie indagini di qualsiasi genere riconosce l'importanza e l'utilità di una prova

[22] G. Amato, V. Destito, G. Dezzani, C. Santoriello, *Op. Cit.* pag. 123 e ss.
[23] Chang-Tsun Li, *Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions*, Information Science Reference, 2010.

informatica per le sue peculiarità, ma soprattutto per l'elevato numero di informazioni che possiamo trovare al suo interno[24].

Il punto di partenza dell'indagine è pressoché identico a quello di un'indagine classica, ossia si cercano di rilevare possibili fonti di prova attraverso l'ispezione della scena del delitto. Una volta individuati dispositivi informatici-telematici interviene il forenser che a seconda della situazione agirà di conseguenza. Infatti la prima cosa a cui badare è capire che tipologia di sistema dobbiamo analizzare (PC fisso, laptop, tablet, smartphone e ecc.) e in secondo luogo se questo è acceso o spento. Ma giuridicamente com'è possibile capire se ci troviamo di fronte ad sistema-informatico o ad un semplice apparecchio elettronico? Ci vengono in aiuto in questo caso due sentenze della Corte di Cassazione, la n. 31135 del 6 luglio 2007, emessa dalla Sezione V penale , e la n. 3067 del 14 dicembre del 1999, emessa dalla Sezione VI Penale. In particolare in quest'ultima viene statuito che può essere considerato "*sistema informatico*" «[…] *una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche. Queste ultime, come si è rilevato in dottrina, sono caratterizzate dalla registrazione (o "memorizzazione"), per mezzo di impulsi elettronici, su supporti adeguati, di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit) numerici ("codice"), in combinazioni diverse: tali "dati", elaborati automaticamente dalla macchina, generano le informazioni costituite "da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente*»[25]. Appurato ciò, il primo esame essenziale che viene effettuato è per determinare se e con quale modalità dovrà avvenire prima la perquisizione ed eventualmente il sequestro del supporto fisico. Effettuare il sequestro probatorio non sempre può essere agevole o efficace (si pensi ad esempio ai mainframe di un azienda che spesso occupano diversi metri quadrati e quindi difficoltosi da spostare e trasportare), quindi la scelta ottimale potrebbe essere quella di effettuare una perquisizione del sistema informatico in loco con le dovute precauzioni. In questo caso se il sistema sarà

[24] F. Cajani, S.Aterno*, Aspetti giuridici comuni delle indagini informatiche*, in S.Aterno, F.Cajani, G. Costabile, M. Attiucci, G. Mazzaraco, *Computer forensic e indagini digitali*, Experta, 2011.
[25] Cass. Pen. Sez. IV, Sent. n. 3067 del 14 dicembre 1999.

acceso si cercherà di fare una copia di back-up dei dati rilevanti o se necessario dell'intero hardware (spesso la scelta è anche dettata dalla mole di dati da essere sottoposta a controllo; prendendo sempre ad esempio i mainframe essi possono contenere diverse centinaia di terabyte. Se volessimo fare un paragone con il mondo fisico immaginate di dover controllare tutte le pagine di tutti i libri di una biblioteca nazionale, un lavoro decisamente troppo lungo e dispersivo). In queste situazioni dove si può facilmente perdere la bussola su cosa sia rilevante copiare o meno, vengono in aiuto diversi programmi o software creati appositamente per ricercare parole chiave, immagini sensibili e via discorrendo. Se invece il supporto fisico è spento per certi versi il forenser può operare con più facilità avendo anche diverse possibilità sul come agire. Il bivio fondamentalmente è tra accendere il sistema e procedere alla perquisizione o alla eventuale copia dei dati, oppure effettuare le suddette operazioni con il sistema spento operando da remoto con specifici apparecchi. Per quanto riguarda la prima scelta c'è sempre il rischio che con l'accensione del dispositivo si inneschino dei programmi di "*pulizia*". Ciò comporterebbe l'eliminazione dei dati o comunque la loro inutilizzabilità (anche se come si dirà nell'apposito paragrafo oggi esistono tecniche che in casi estremi permettono di recuperare dati che si pensavano persi). E' necessaria quindi un'azione preventiva che permetta di esaminare i diversi File in tranquillità, per esempio utilizzando software che operano durante l'accensione permettendo di non essere individuato dal sistema. Tuttavia, a meno che per particolari esigenze non si è costretti ad accendere il sistema, solitamente si preferisce operare con il dispositivo spento, essendo quest'ultimo incapace di reagire alle perquisizioni telematiche degli inquirenti. Oltretutto accedendo ai file direttamente con il PC acceso spesso si rischia di inquinare, come nella vita reale d'altronde, le aeree virtuali a cui si accede (si pensi ad esempio alla cronologia di visita del sistema, dei siti internet o delle modifiche apportate ai file), mentre da remoto si può procedere alla sola lettura dei file senza intaccare il sistema e lasciare tracce. Vediamo ora com'è possibile esaminare un PC, uno smartphone, un tablet e ecc. se quest'ultimi sono inattivi o spenti, oppure non si vuole correre il rischio di accenderli e perdere preziose informazioni.

2.1.1 *La copia forense e i mezzi per ottenerla*

Qualora si presenti il caso di una situazione in cui il sistema informatico è spento o comunque non è possibile attivarlo per svariate ragioni, e si vuole procedere con una certa cautela, ci viene in soccorso il progresso tecnologico con due particolari dispositivi: il "*block writer*" e/o i duplicatori forensi.

I "*block writer*" «*sono apparati che permettono di accedere alla memoria di massa garantendo la modalità di solo lettura a livello hardware*»[26], solitamente a livello materiale somigliano a degli hard disk con un cavo che si può collegare direttamente al sistema o alla memoria di massa di quest'ultimo. Attraverso il block writer è possibile entrare furtivamente nel sistema senza creare alterazioni di alcun tipo. Il limite di tale strumento è quello di poter ispezionare i diversi file solo attraverso un controllo in loco, oppure se sequestrato l'intero dispositivo con successivi controlli in laboratorio.

Per quanto riguarda invece i "*duplicatori forensi*" «*eseguono una copia in bit-stream dell'unità di memoria rilasciando un opportuno certificato*»[27], e al contrario del block writer il duplicatore non fa accendere al sistema senza lasciare traccia, ma clona il contenuto della memoria del dispositivo bit per bit. Il termine clonare non è scelto a caso. Infatti, sebbene la si possa anche definire "*copia forense*", quella che viene eseguita è una vera e propria duplicazione della sorgente senza sconvolgere la posizione dei dati o effettuare la loro compressione come potrebbe avvenire con un semplice copia e incolla. Addirittura vengono pure duplicati i cosiddetti dati fantasma ossia quei dati non visibili direttamente all'utente e che stanno solitamente in zone dette "*aree non allocate*". In sostanza quindi, volendo fare un parallelismo con le fonti di prova del mondo fisico, la copia forense più che alla copia di un documento[28] (che tra l'altro nel mondo virtuale, insieme al concetto di originale, perde di significato) può essere paragonata ad una fotografia, visto che la rappresentazione dei dati ottenuta dall'inquirente è pedissequa a quella originale. E' proprio per questo che spesso

[26] G. Amato, V. Destito, G. Dezzani, C. Santoriello, *Op. Cit*., pag. 188.
[27] L. Luparia ,G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, 2007;
G. Amato, V. Destito, G. Dezzani, C. Santoriello, *Op. Cit.*
[28] Cass. Pen. Sez. V, Sent. n. 6887 del 13 aprile 1999;
Cass. Pen. Sez. V, Sent. n. 5337 del 16 marzo 1999.

nelle varie direttive internazionali, linee guida e "*best practice*" viene preferita rispetto ad altri metodi o strumenti, per il semplice fatto che (come vedremo nell'apposito paragrafo sull'acquisizione e valutazione delle prove) garantisce una copia asettica e priva di ingerenze esterne e permette di fatto un'analisi peritale altamente certificata. In ambito di prove informatiche, in particolare sulle copie forensi, si è espressa anche la nostra Corte di merito, fornendo delle precisazioni con la sentenza n. 954/09. Secondo il giudice «*per atto irripetibile deve intendersi l'atto contraddistinto da un risultato estrinseco ed ulteriore rispetto alla mera attività investigativa, non più riconducibile in dibattimento se non con la perdita dell'informazione probatoria o della sua genuinità. Sotto tale profilo gli accertamenti ex art. 360 c.p.p. consistono in attività di carattere valutativo su base tecnico scientifica e non in attività di constatazione, raccolta, prelievo dei dati materiali pertinenti al reato*. […] *Ciò posto, è da escludere che l'attività di estrazione di copia di "file" da un computer costituisca un atto irripetibile* (nel senso in precedenza indicato), *atteso che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica né determina alcuna alterazione dello stato delle cose, tale da arrecare pregiudizio alla genuinità del contraddittorio, conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale*»[29]. Una massima non indifferente quindi, soprattutto se si combina questa ratio con la certezza e l'affidabilità delle procedure di best practice che garantiscono l'integrità e l'autenticità del dato informatico e la sua valenza all'interno del processo garantita anche da altre pronunce della Corte[30].

Si sono esaminati finora i casi in cui i dispositivi fossero o accesi o spenti preferendo effettuare le perquisizioni a sistema spento. C'è da precisare però che qualora il sistema venga ritrovato acceso, sempre ad eccezione di particolari esigenze di circostanza, non è consigliabile procedere allo spegnimento, ancor peggio forzato. Una prassi piuttosto frequente nel passato era quella che al rinvenimento di un PC acceso si dovesse scollegare il cavo di alimentazione o togliere la corrente, soprattutto in previsione di un eventuale sequestro. Oggi si potrebbe dire che gli inquirenti sono abbastanza divisi su questo approccio,

[29] Cass. Pen. Sez. I, Sent. n. 954 del 5 marzo 2009.
[30] Cass. Pen. Sez. I, Sent. n. 14511 del 5 marzo 2009.

nonostante la maggior parte delle direttive ormai ha abbandonato questo "*modus operandi*"[31].

Si è detto che accendere un dispositivo spento potrebbe avviare software pericolosi per l'integrità dei dati, la stessa cosa può avvenire con il procedimento inverso, ossia spegnendo il sistema in maniera ordinaria. Da questo timore era nata l'abitudine di scollegare tutto manualmente in maniera tale da impedire qualsivoglia attivazione di programmi dannosi. Tuttavia se da una parte ciò garantisce una certa sicurezza nella fase di spegnimento rispetto a quello ordinario, dall'altra si possono creare ulteriori problematiche da non sottovalutare. Innanzitutto, quando un dispositivo elettronico viene privato di colpo della corrente, avviene all'interno di esso un calo di tensione che potrebbe danneggiare i cip e di conseguenza il dispositivo stesso, potendo portare a un suo successivo inutilizzo. Se poi in particolar modo ci troviamo di fronte ad un dispositivo informatico, con lo spegnimento forzato è pur vero che non si darebbe il tempo ai software malevoli di intervenire, ma non si attiverebbero neanche i protocolli standard di quando un sistema viene chiuso, come salvare i dati ancora in RAM (la memoria volatile che non viene adibita alla conservazione dei file ma che permette di eseguire diverse operazioni ad una certa velocità e in determinate quantità), salvare la cronologia dei siti internet eventualmente ancora aperti, chiudere file aperti (che con lo spegnimento forzato verrebbero danneggiati). Facendo in breve una summa dell'operazione i bonus potrebbero essere nettamente inferiori rispetto ai malus, sicché ad oggi si preferisce, a fronte sempre di casi estremi, operare delle chiusure manuali non forzate utilizzando programmi che permettano uno spegnimento sicuro del sistema senza causare danneggiamenti di ogni sorta.

2.1.2 *Una prassi consolidata: il sequestro "non indiscriminato"*

Ulteriore prassi oggi adottata è quella del sequestro "*non indiscriminato*". In passato spesso si procedeva a sottoporre a sequestro probatorio tutto ciò che

[31] O. Signorile, *Computer Forensic Guidelines: un approccio metodico – procedurale per l'acquisizione e analisi delle digital evidence*, in *Ciberspazio e Diritto*, Mucchi editore, 2009.

poteva essere collegato ad un sistema informatico. Inutile dire che questa procedura era logicamente un inutile dispendio di energie, essendo, per esempio, molte componenti di un dispositivo superflue ai fini delle indagini informatiche (si pensi ad un caso in cui sia coinvolto un intero personal computer. Strumenti come il monitor e le casse audio sono semplici strumenti di out-put, che non possono contenere informazioni rilevanti per un forenser, oppure se il sistema fosse stato utilizzato da più persone appropriarsene significherebbe danneggiare anche altri indiscriminatamente compromettendo anche la loro privacy). L'obiettivo primario è quello di recuperare più dati e file di interesse, ragion per cui il sequestro deve essere rivolto essenzialmente a quei supporti di memorizzazione di cui è possibile una sicura rimozione senza perderne il contenuto, come CD-ROM, memorie USB, mini hard disk e ecc. o ancora più nello specifico a singoli file Fondamentalmente ad oggi il sequestro di un intero hardware viene giustificato solo nel caso in cui quest'ultimo sia stato utilizzato in toto per commettere attività illecite (caso non molto raro)[32], oppure, se non è indispensabile operare il sequestro si preferisce eseguire le dovute copie in loco mantenendo la scena del crime più intatta possibile. Da un punto di vista normativo per l'effettuazione del sequestro non ci sono particolari differenze da un sequestro classico. Di conseguenza in base all'art. 250 c.p.p. sarà possibile per il destinatario dell'atto partecipare al sequestro anche tramite proprio difensore o una persona di fiducia, senza diritto però ad un preavviso. Inoltre dovranno essere osservate anche le disposizioni contenute negli artt. 81-82 disp. att. c.p.p. in merito alla redazione del verbale con indicate tutte le operazioni effettuate per il deposito e la custodia dei diversi elementi di prova e di come verrà garantita la loro integrità e impedirne la modificabilità attraverso i certificatori o duplicatori forensi[33].

Un punto di svolta è stato reso con un'ordinanza emessa il 4 ottobre del 2006 dal Tribunale di Brescia che stabilisce che «*il sequestro di un intero hard-disk consente certamente l'acquisizione di elementi probatori, ma implica anche l'acquisizione di dati che esulano dal contesto per il quale l'atto e disposto,*

[32] G. Amato, V. Destito, G. Dezzani, C. Santoriello, *Op. Cit*. pag. 127.
[33] A. Macrillo', *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. Internet*, 2008, Ipsoa.

sicché, come è immediatamente percepibile, tale genere di sequestro esige un ambito di corretta e ristretta operatività per evitare connotazioni di spropositata afflittività e di lesione di beni costituzionalmente protetti. Sotto questo profilo merita particolare segnalazione la compressione della libertà e segretezza della corrispondenza conservata nel disco fisso, con conoscenza dei messaggi tutti trasmessi e ricevuti, compresi quelli destinati a soggetti del tutto estranei alle indagini»[34]. Tuttavia, sebbene ciò che viene affermato nell'estratto presenta punti di svolta decisivi per la computer forensics italiana, ci troviamo di fronte ad una giurisprudenza che di certo non ha e non aveva il peso per influenzare il legislatore ha prendere provvedimenti adeguati in merito. In seguito la giurisprudenza di legittimità della Cassazione[35] (nella quale verrà stabilito che anche nell'ambito informatico vi deve essere «*proporzione tra il contenuto del provvedimento emesso e le esigenze di accertamento dei fatti [che] deve avvenire con particolare rigore, evitando quanto più possibile interventi inutilmente invasivi*»), insieme alla legge 48/2008, chiarificherà diversi dubbi che erano sorti sulla questione, ponendo fine alle lacune iniziali. Difatti, anche le più recenti decisioni giurisprudenziali[36] tendono oggi a valutare il sequestro indiscriminato come un approccio decisamente obsoleto e superfluo, poiché viene reiterato che spesso si viola il principio di proporzionalità ed adeguatezza, rendendo quindi ogni volta gli elementi di prova acquisiti non idonei a formare il giudizio del giudice.

2.1.3 *La ricerca delle fonti di prova, in particolare cellulari, smartphone e PDA*

Si è analizzato finora il caso classico in cui oggetto dell'indagine degli inquirenti sia un personal computer (che per analogia possiamo estendere anche alla situazione in cui siano coinvolti dei pc portatili laptop o notebook), ma si è già detto che questi oggi comprendono solo una parte dei mezzi informatici utilizzati dalla gente comune, anzi ad essere sinceri il dispositivo di più diffuso

[34] Trib. di riesame di Brescia Sez. II, Ordin. n. 11972 del 4 ottobre 2006.
[35] Cass. Pen. Sez. I, Sent. n. 25766, del 16 febbraio 2007.
[36] Cass. Pen. Sez. VI, Sent. n.24617 del 24 febbraio 2015.

utilizzo è il telefono cellulare. La trattazione di quest'ultimo potrebbe esulare da questi tesi se guardassimo al cellulare come un telefono mobile classico, quando in verità la sua fisionomia e le sue funzioni sono cambiate parecchio con gli anni. Infatti il termine più corretto con cui identificare questi apparecchi sarebbe quello di telefoni intelligenti e PDA, con componenti e processori tipici di veri e propri mini computer. Questi sistemi hanno sia il vantaggio della più ampia portabilità, essendo perlopiù tascabili, sia le capacità prestazionali di un discreto pc potendo immagazzinare diverse quantità di dati (per dare dei dati concreti i moderni cellulari possono arrivare fino a 128 Gb di memoria per non parlare dei mini-tablet che possono superare facilmente questa soglia). In aggiunta questi dispositivi sono sempre dotati anche di una scheda SIM che permette all'utente di usufruire del servizio telefonico.

Il NIST (National Institute of Standards and Technology) ha classificato i telefoni cellulari principalmente in tre categorie:

«1) *Basic phone, ovvero un terminale radiomobile con velocità di calcolo e memoria limitata, dotato di uno schermo in scala di grigi, privo di fotocamera e scheda di memoria aggiuntiva, utilizzato per chiamate ed invio di messaggi di testo, collegabile ad un computer tramite cavo o infrarosso, con una batteria ricaricabile al litio e senza la possibilità di connettersi ad internet per la navigazione web e l'invio della posta elettronica;*

2) *Advanced phone, ovvero un terminale radiomobile con velocità di calcolo e memoria superiore, dotato di uno schermo in scala di colore, equipaggiato con una fotocamera a bassa risoluzione e dotato di un alloggiamento per schede di memoria aggiuntive, utilizzato per chiamate, invio di messaggi di testo e agenda per gli appuntamenti, collegabile ad un computer tramite cavo, infrarossi o bluetooth, con una batteria ricaricabile al litio ed in grado di collegarsi ad internet a velocità limitata per la navigazione Wap e l'invio e la ricezione di posta elettronica*;

3) *Smart phone, ovvero un terminale radiomobile dall'elevata capacità di calcolo e di memoria, dotato di uno schermo a colori reali, equipaggiato con una fotocamera ad alta risoluzione in grado di riprendere anche filmati, con la possibilità di contenere memorie di massa o rimovibili aggiuntive ad alta*

capacità, utilizzato per chiamate, invio di messaggi di testo o multimediali e agenda degli appuntamenti, collegabile ad un computer tramite cavo, infrarosso, bluetooth e Wi-Fi, con una batteria ricaricabile al litio ed in grado di collegarsi ad internet ad alta velocità per la navigazione Web, l'invio e la ricezione di posta elettronica e l'istant messaging»[37].

Guardando quindi agli smartphone con un punto di vista puramente investigativo, essi sono una fonte di prova particolarmente interessante per il semplice fatto che sono un enorme ricettacolo di informazioni anche di diversa natura tra di loro (si pensi alle immagini e file salvati, numeri di telefono degli ultimi contatti, messaggi, tracciati GPS e ecc.). I cellulari posso essere classificati anche da un punto di vista di elettronico o di rete, anche se oramai tutti dispositivi di vecchia generazione, basati su tecnologia analogica, sono stati ritirati per permettere una maggiore diffusione dei modelli 4G. Avendo presente ciò, ed in collegamento con quanto detto prima, affinché un dispositivo mobile possa connettersi alla rete e/o chiamare è necessaria «*una particolare "smart card" detta Subscriber Identity Module (SIM). Tale scheda consente di identificarsi nella rete del provider che l'ha rilasciata. Una SIM è caratterizzata da due codici:*

- *Integrated Circuit Card Identification (ICCID), ovvero un codice di venti cifre che la identifica unicamente quale hardware.*
- *International Mobile Subscriber Identity (IMSI), ovvero un codice di cinque cifre memorizzato all'interno della SIM e composto da tre parti:*
    - *Mobile Country Code (MCC), che rappresenta il codice della nazione;*
    - *Mobile Network Code (MNC), che rappresenta il codice di rete;*
    - *Mobile Station Identification Number (MSIN), che rappresenta il numero univo dell'utente all'interno della rete del suo operatore.*

[37] M. Epifani*, Analisi di telefoni cellulari in ambito giuridico*, in *Ciberspazio e Diritto*, 1, 2009, pag. 83-84.

Alcuni terminali radiomobili di ultima generazione possono integrare al loro interno due schede SIM. Questo consente di associare ad unico dispositivo più numeri di telefono attivi contemporaneamente»[38].

2.1.4 *L'analisi nello specifico di cellulari e smartphone*

Quando in una "*scena criminis*" viene reperito un cellulare essenzialmente la sua analisi si muoverà su quattro settori: memoria interna, memoria esterna removibile, la scheda SIM ed infine il provider della rete mobile che fornisce il servizio di accesso alla rete. La procedura adottata nei confronti di questi apparecchi è simile a quella per i PC, ossia cercare di operare possibilmente con il sistema spento per evitare danneggiamenti o reazioni indesiderate ed effettuare delle copie certificate della memoria interna. Essendo i contenuti riscontrabili all'interno tra i più disparati, di solito durante la duplicazione vengono effettuati dei report in maniera tale da suddividere i dati acquisiti con un certo ordine a seconda di dove sono stati presi (ad esempio messaggi di posta, file multimediali, file cancellati e ecc.), ed infine viene garantito che rimangano immodificati attraverso le apposite metodologie. L'analisi inizia appunto dalla memoria di base interna del cellulare. Da quest'ultima è possibile innanzitutto apprendere diverse specifiche del telefono, come tipologia, modello e altre caratteristiche tecniche. Questo è un ottimo punto di partenza per poi recuperare tutto ciò che è all'interno della memoria come numeri, sms, mms, foto, video audio, documenti word, email, conversazioni da applicazioni di messaggistica e ecc.

Per quanto riguarda l'analisi che comprende la scheda SIM è di certo molto più breve ma non meno importante. Infatti queste schede hanno una capacità di memoria molto limitata (i modelli 128K possono arrivare a contenere un massimo circa di 32 Megabyte, che in termini pratici sono mezzo migliaio di contatti telefonici ed una cinquantina di sms), ma spesso possono conservare informazioni che il reo pensava di aver eliminato dal cellulare, ma che invece sono rimaste in memoria nella SIM. La scheda può essere trasferita da cellulare a cellulare a

[38] M. Epifani, *Op. Cit.,* pag. 84.

seconda del suo formato (standard, mini, micro), ciò rende possibile quindi che il supporto possa immagazzinare diversi dati eterogenei, ma che possono costruire una cronologia di quelli che sono stai i movimenti del soggetto agente, dato che è possibile recuperare, oltre che parte della rubrica, messaggi e le ultime telefonate, anche la posizione dell'ultima cella a cui il telefono si è collegato l'ultima volta che lo si è utilizzato. Inoltre tramite quest'ultima è possibile risalire sia al tipo di contratto sia all' operatore di telefonia mobile che il proprietario del telefono ha utilizzato. Una volta ottenute queste informazioni è possibile risalirne a molte altre, come l'identità del soggetto che ha stretto il contratto, ed eventualmente se è stata fatta denuncia di furto, da quando il numero telefonico è attivo, promozioni, movimenti, tabulati e via discorrendo. Tuttavia se da una parte la presenza di una scheda SIM all'interno di un dispositivo mobile cellulare può rivelarsi utile sotto molto aspetti, dall'altra bisogna anche considerare i lati negativi che potrebbe comportare la presenza di quest'ultima. Questo perché le SIM garantiscono anche un certo livello di sicurezza attraverso la possibilità per l'utente di impostare due codici di accesso: Il codice PIN ("*Personal Identification Number*") e il codice PUK ("*Personal Unlocking Key*"). Il primo può essere composto da un minimo di quattro ad un massimo di otto numeri, è personalizzabile dall'utente, e viene richiesto ogni qualvolta si accende il cellulare. Il secondo è un codice di sblocco di emergenza nel caso in cui si sbagli ad inserire per un certo numero di volte, solitamente tre, il codice PIN ed è composta da dieci cifre. Qualora si sbagli anche l'inserimento del PUK la scheda si blocca e non più possibile recuperare i dati su di essa. Quindi potrebbe accadere che per fare perdere informazioni compromettenti all'interno della SIM, il possessore del dispositivo volontariamente blocchi il proprio telefono ed in seguito ne tenti la distruzione. In tal caso l'intervento del forenser è piuttosto limitato dato che ad oggi non esistono "*tools*", sia in formato fisco che di programma, che permettano di oltrepassare, decifrare o aggirare le restrizioni imposte da questi codici, sicché in caso di blocco, a meno che non si conosca il codice, quelle informazioni sono perse per sempre[39].

[39] E. Casey, *Handbook of computer crime investigation. Forensic tools and technology*, Acadamic Press, 2003.

I cellullari sono spesso dotati di appositi vani dove è possibile inserire "*memory card*" esterne. Questi supporti, che solitamente si dividono in SD (*Secure Digital*), mini SD e micro SD a seconda della dimensione fisica, possono essere molto piccoli (all'incirca della grandezza di un unghia del mignolo), ed avere allo stesso tempo un'elevata capacità di immagazzinamento e lettura di dati fino a 512 GB. Da un punto di vista investigativo l'analisi di una scheda di memoria è comunque di un certo interesse visto che può contenere diverso materiale probatorio digitale come foto, video, tracce audio e ecc., proprio come la memoria flash del cellulare, con l'ulteriore caratteristica che, al contrario di quest'ultima, è estraibile, quindi può essere nascosta oppure essere usata per nascondere qualcosa facilmente, e può essere letta oltre che dai dispositivi compatibili anche da un computer con appositi adattatori.

Infine per ultimo, ma non meno importante, dobbiamo considerare il possibile recupero di informazioni e dati attraverso il gestore telefonico del traffico di dati, poiché «*con le opportune autorizzazioni è possibile richiedere informazioni utili all'indagine direttamente al Network Service Provider. Il D.Lvo 109/2008 ha introdotto le specifiche delle informazioni che il fornitore deve conservare. In particolare, in ambito di comunicazioni telefoniche cellulari, i dati che si possono ottenere dal provider sono:*

- *Numero telefonico chiamante*
- *Nome e indirizzo dell'utente registrato*
- *Numero composto, ovvero il numero e i numeri chiamati, e nei casi di servizi supplementari, (come inoltro o trasferimento di chiamata) il numero i numeri verso i quali è diretta la chiamata*
- *Nome e indirizzo dell'abbonato o dell'utente registrato*
- *Data e ora dell'inizio e della fine della conversazione*
- *IMSI del chiamante e del chiamato*
- *IMEI del chiamante e del chiamato*
- *Etichetta di ubicazione (Cell ID) all'inizio della comunicazione.*»[40]

[40] M. Epifani, *Op. Cit*., pag. 86-87.

Tutte queste informazioni sono molto utili sia all'interno di processo penale per poter ricostruire un alibi, una cronologia degli eventi o semplicemente convalidare o smentire affermazioni fatte da un testé oppure dallo stesso imputato, sia agli inquirenti durante le stesse indagini per avere punti di svolta e risalire ai soggetti coinvolti o collegati ad un reato.

Nonostante abbiamo delineato uno standard minimo di azione, in realtà esistendo diverse tipologie di smartphone e tablet non vi è una procedura univoca per tutti, ma dipende dal supporto che ci troviamo di fronte, potendo su alcuni sistemi funzionare meglio un block writer o su altri un software o un programma di analisi forense. Per la precisione ciò che può influenzare l'analisi di un dispositivo mobile sono il sistema operativo e i programmi installati su di esso, nonché le abilità e gli strumenti a disposizione dell'investigatore. In ogni caso, anche con le dovute accortezze, ci troviamo in un territorio complesso. L'eterogeneità dei dati e della loro destinazione rendono difficili i classici approcci del forenser, sicché è più opportuno muoversi con logica e quindi effettuare copie forensi mirate e specifiche e non "*bit for bit*". Nel momento in cui il dispositivo viene rinvenuto, prima di procedere al sequestro, si effettuano le stesse operazioni preliminari che per qualsiasi dispositivo elettronico informatico, ossia si prende nota nel verbale delle condizione di ritrovamento (posizione, danni, eventuali segni e altre tracce organiche) e se possibile si documenta il tutto con fotografie della "*scena criminis*". Una volta che si ha un quadro chiaro della situazione si procede all'analisi, e anche qui, come nell'analisi dei PC, si aprono due bivi a seconda delle circostanze. Una prima distinzione sul modo di agire è basata sull'integrità del cellulare al momento del sequestro. Se quest'ultimo è parzialmente o completamente distrutto, o comunque è stato reso inutilizzabile, si dovrà procedere necessariamente all'estrazione della memoria interna ed effettuare una ricerca in separata sede in laboratorio. Nei casi più gravi di manomissione occorrerà invece il supporto di tecnici specializzati, poiché è probabile che si debba effettuare una ricostruzione dell'hardware o comunque dei dati leggibili che si possono recuperare. Qualora invece il dispositivo dovesse essere in buono stato o comunque uno stato tale che permetta di effettuare le normali operazioni forensi, si procede in maniera differente a seconda che il dispositivo sia acceso o spento:

se il dispositivo è acceso, come per qualsiasi altro terminale informatico, gli inquirenti si trovano in una posizione di vantaggio investigativo, dato che ancora possono recuperare non solo ogni dato presente nella RAM, ma anche reperire informazioni che a telefono spento non sarebbero reperibili. Tuttavia nell'analisi di un telefono cellulare acceso si prospettano due problematiche, le quali, se il forenser non interviene prontamente, possono comportare la compromissione dell'intera indagine per inquinamento probatorio, e quindi l'acquisizione di elementi di prova non idonei a formare il convincimento del giudice e su cui quest'ultimo non può fondare la sua decisione. Se il dispositivo mobile è attivo, innanzitutto bisogna provvedere a che la batteria non si scarichi e quindi si spenga. In seguito bisogna schermare il cellulare in maniera tale che, come nei PC collegati alla rete, possano avvenire ingerenze esterne. Al primo problema si può ovviare facilmente attraverso l'utilizzo di un carica batterie universale, ancora meglio se quest'ultimo è portatile o a batterie e quindi non necessita di una presa di corrente. Il secondo inconveniente invece è più complesso, ma presenta diverse soluzioni. Secondo un' autorevole dottrina[41] il miglior approccio, nonché quello più utilizzato dagli inquirenti, è quello di effettuare l'analisi e la ricerca dei dati all'interno di una gabbia di Faraday (una stanza o un contenitore materiale attraversato da corrente che impedisce l'intromissione di qualsiasi campo elettrostatico o elettromagnetico esterno). Attraverso la gabbia è possibile sia trasportare sia analizzare il telefono con la sicurezza che, grazie al campo elettromagnetico che fa da schermo, non sarà possibile in nessun modo ricevere intromissioni, non potendo il segnale di rete raggiungere in nessun modo il dispositivo. Tuttavia questa tecnica non esente da aspetti negativi. Il continuo sottoporre il cellulare a un campo elettromagnetico, che impedisce di prendere segnale, porta il terminale mobile ad uno sforzo energetico considerevole per la sua ricerca che potrebbe scaricare la batteria in tempi molti brevi. La migliore accortezza in questo metodo quindi è quello di tenere costantemente collegato ad un carica batterie il dispositivo in maniera tale da impedirne lo spegnimento, soprattutto durante il trasporto di quest'ultimo dal luogo del delitto fino al laboratorio forense.

[41] M. Epifani, *Op. Cit.*, pag. 89.

Come già detto prima però esistono anche altre soluzioni abbastanza valide, che tuttavia sono da considerare in secondo piano qualora si possa disporre della gabbia di Faraday. Un sistema ancora più sofisticato e sicuro, ma che comporta un maggior dispendio di risorse economiche (il quale lo rende un mezzo di per sé poco utilizzato dalle diverse Procure) e di restrizioni a livello giuridico, è l'utilizzo di un "*jammer*", ossia un disturbatore di frequenza. Sebbene «*un jammer device è sicuramente più efficace per garantire la conservazione delle informazioni sul telefono e l'integrità della prova, tuttavia gli utilizzi impropri di questi dispositivi violano la legge 98/1978, gli Artt. 615 bis, 617, 617 bis c.p. e l'Art. 226 bis c.p.p. sulla riservatezza della vita privata e le intercettazioni delle comunicazioni*»[42]. Un altro metodo è quello di mettersi in contatto con il Provider del gestore telefonico e chiedere di attivare l'isolamento del cellulare. Questa potrebbe essere ritenuta la scelta migliore sul campo se non per il fatto che ha tempi di attivazione piuttosto lunghi. Affidarsi unicamente a questa possibilità quindi porterebbe sempre e comunque a dei rischi notevoli, non essendo prevedibile cosa possa succedere nell'intervallo di tempo tra l'effettuazione della richiesta della sospensione del servizio e la sua attivazione concreta. Infine l' ultima modalità d'azione del forenser nei confronti di un cellulare acceso è quello di reperire dati e informazioni attraverso un approccio diretto al dispositivo senza utilizzo di "tools" particolari, ma anche questa pratica presenta diversi rischi[43]. Se da una parte può essere un metodo molto immediato e veloce, dall'altra si potrebbe compromettere la validità degli elementi di prova per modifiche o cancellazioni dei file. In definitiva si tende ad effettuare questa analisi solo come *estrema ratio*, e comunque è richiesta dall'investigatore una grande abilità e conoscenza del terminale mobile che ha ad oggetto, che comunque prima di ogni operazione dovrà effettuare prove su un dispositivo analogo a quello ritrovato e documentare il tutto tramite audio-video.

Nel caso in cui invece il dispositivo viene rinvenuto spento, oppure per cause di forze maggiore o per causalità si è reso necessario lo spegnimento, bisognerà muoversi diversamente. Nonostante il terminale mobile sia inattivo, seppur minimo, vi è un consumo di energia, quindi anche in questo caso sarà doveroso

[42] M. Epifani, *Op. Cit*., pag. 89.
[43] D. Schweitzer, *Incident Response: Computer Forensics Toolkit*, Wiley, 2003.

collegare il cellulare ad un caricabatteria, in maniera tale da evitare che vada "*sottosoglia*", si ravvii e si perdano in definitiva informazioni utili che era possibile trarre dalle impostazioni configurate dall'utente. Le vie percorribili a questo punto sono due:

La prima consiste nel provare ad accendere il telefono. Una procedura inversa a quella che avviene nell'analisi di un PC, per il semplice fatto che difficilmente, anche se si tratta di *smartphone*, possano essere presenti programmi di cancellazione e pulizia che si avviino all'accensione. Tuttavia la maggior parte delle volte si riscontra la problematica di dover inserire o il codice PIN o il codice PUK. In tal caso si deve provare a recuperarli attraverso richiesta all'operatore telefonico che gestisce il servizio o, se è stato modificato, da ciò che viene detto dall'indagato in fase di interrogatorio o dagli altri indizi o elementi di prova sul *locus commissi delicti*. Se l'esito delle indagini è negativo, comunque sia deve rimanere almeno un tentativo valido di inserimento del PIN, o quanto meno del PUK. Questo appunto per evitare di perdere sia in definitiva i dati sul dispositivo, sia la possibilità di poter recuperare con indagini future quei codici.

La seconda via prevede la creazione di una SIM clone e ad oggi è l'approccio prediletto da diversi pareri dottrinali[44]. Attraverso questo metodo viene creata una copia perfetta della SIM originale all'interno del terminale mobile sequestrato. Piccolo inconveniente, ma non irrilevante, è che così facendo si disattiva la precedente scheda e si potrebbe perdere tutto il suo contenuto, se non si interviene prontamente con appositi software di recupero.

In ogni caso punto fondamentale di ogni indagine che coinvolga un cellulare è quello di collegare ad un PC il cellulare per effettuare una scansione ed un'analisi più accurata ed eseguire la "*virtualizzazione*"[45] del dispositivo su cui si è operato. In questo modo viene ricreato, anche se non fisicamente, il dispositivo hardware soggetto ad esame completo anche di software operativo, in maniera tale da poter eseguire in sicurezza vari test sulle diverse azioni praticabili su quell'apparecchio (ad esempio come e dove vengono salvati e/o cancellati i dati). Inoltre se possibile

[44] F.Casadei, A.Savoldi, P.gubian, "*Forensics and SIM cards: an Overview*", in *International Journal of Digital Evidence*, 2006, Volume 5, Issue 1;
M. Epifani, *Op. Cit*.

[45] G. Amato, V. Destito, G. Dezzani, C. Santoriello, *Op. Cit*., pag. 180.

viene anche effettuata una simulazione "*on-line*" cercando di riprodurre anche lo stesso tipo di configurazione e collegamento alla rete.

2.1.5 *Le indagini nell'ambito informatico e l'oscuramento dei siti internet*

Nell'ambito dei reati (informatici e non) sono spesso coinvolti anche siti internet ed in tal caso le indagini sono definite come informatico-telematiche[46]. In tal caso, quando si opereranno delle perquisizioni o delle ispezioni, la notifica dovrebbe avvenire anche essa per via telematica attraverso l'utilizzo di posta elettronica certificata o firma digitale. Unico problema di questa situazione è che non esiste una normativa specifica in merito, e qualora esistesse comunque sarebbe applicabile solo ai server in territorio italiano, lasciando scoperti tutti quei siti che si appoggiano a server esteri fuori dalla nostra giurisdizione e raggiungibili solo attraverso rogatoria internazionale[47]. Ciò non toglie che, essendo possibile comunque utilizzare un sito WEB per compiere reati, quest'ultimo non possa essere soggetto a sequestro probatorio, sia come oggetto pertinente al reato sia come vero e propria fonte di prova. Essendo un sequestro prettamente telematico, solitamente si procede inizialmente con l'oscuramento del sito, in maniera tale da renderlo inaccessibile all'utenza ed impedire il perpetuare dell'azione criminosa (ad esempio un atto diffamatorio oppure la distribuzione di materiale pedo-pornografico).

Anche l'oscuramento col tempo è diventata sempre più un azione selettiva e ben mirata in maniera tale da arrecare il minor disagio possibile, colpendo quindi solo determinate aeree del sito interessato. Una volta che il sito è stato reso innocuo devono essere compiute due ulteriori azioni ben distinte: per prima cosa vengono estratti dal server a cui si appoggia il sito tutti i file di interesse ed eventuali banche dati. Inoltre vengono anche prelevati i log (la registrazione sequenziale e cronologica delle operazioni effettuate da un utente o da un amministratore), così

[46] G. Amato, V. Destito, G. Dezzani, C. Santoriello, *Op. Cit.* pag. 129.
[47] F. Lisi, G. Muraro e A. Nuzzolo, *I reati informati: nuova disciplina e tecniche processuali di accertamento*, Maggioli Editore, 2004, pag. 107.

da poter ricostruire la storia del sito internet e chi ne ha fatto parte; in seguito è necessario garantire l'integrità dei file estratti attraverso le operazioni di certificazione per assicurargli validità probatoria. Infine è prassi allegare un lista stampata dei file da allegare al verbale del sequestro e salvare i file certificati su appositi supporti di memorizzazione immodificabili. Tutta la procedura fin qui descritta non riscontra particolari problemi nel caso in cui il sito WEB si appoggi ad un unico server. In caso contrario sarà più complesso procedere all'oscuramento del sito e alla successiva perquisizione dovendo individuare tutte le diverse fonti di appoggio. Non è raro il caso in cui oggetto dell'indagine e del successivo sequestro possa essere proprio un server. Concettualmente i server non differiscono poi tanto da un qualsiasi sistema informatico composto da hardware e software operativo (come i pc, gli smartphone e ecc.), ma naturalmente rispetto ai dispositivi classici presentano una maggiore complessità nella loro struttura e una maggiore capienza di dati che processano. In tal caso il problema dell'inquirente è fondamentalmente lo stesso di quando deve ispezionare, perquisire o sequestrare un "*main frame*", ossia l'enorme mole di file da sottoporre ad analisi, inoltre i server visto che devono garantire un servizio on-line, sono costantemente accesi e di conseguenza non sarà possibile operare a sistema spento come di solito si consiglia di procedere per gli altri sistemi.

Partendo dalla prima problematica si possono intraprendere due vie[48] [49]:

a) la prima possibilità è quella di rendere sicuro e sterile l'ambiente virtuale attraverso l'utilizzo di programmi specifici attivabili attraverso dei supporti di memorizzazione portatili e che non necessitano di installazione ed in seguito procedere alle duplicazioni forensi. Questi programmi differiscono da quelli solitamente utilizzati nelle normali computer forensics perché sono in grado di attivare i sistemi RAID (una tecnica di raggruppamento di diversi dischi rigidi collegati ad un computer che li rende utilizzabili come se fosse un unico volume di memorizzazione garantendo, rispetto ad un disco singolo, incrementi di prestazioni, aumenti nella capacità di memorizzazione

[48] F. Lisi, G. Muraro e A. Nuzzolo, *I reati informatici: nuova disciplina e tecniche processuali di accertamento*, Maggioli Editore, 2004.
[49] G. Amato, V. Destito, G. Dezzani, C. Santoriello , *Op. cit.*, pag. 139.

disponibile e miglioramenti dei malfunzionamenti) su cui di solito sono montati la maggior parte dei server.

b) La seconda possibilità prevede invece di effettuare una ricostruzione del server in laboratorio attraverso l'unione delle singole copie effettuate dal sistema RAID. Quest'ultima scelta è quella solitamente preferita dagli inquirenti anche se comporta la premessa di base che si disponga dei mezzi adeguati a ricostruire il server e che la ricostruzione sia identica all'originale.

La seconda problematica nel recupero dei dati attiene al fatto che il server è operativo H24 e che viene costantemente aggiornato sia dagli amministratori che dagli utenti, cambiando continuamente i file al suo interno. Ciò premesso è necessario quindi scollegare il server dalla rete in modo da cristallizzare lo status di quest'ultimo, disattivando la scheda di rete e rimuovendo i cavi, inoltre l'operazione che verrà eseguita, per forza di cose, sarà irripetibile.

Infine ultimo ostacolo che si può incontrare nel sequestro di un server è l'esagerato numero di dati che si devono analizzare (che come già detto in merito ai main frame possono raggiungere diverse centinaia di Terabyte rispetto agli hard disk comuni). In tal caso, come per l'analisi dei PC, l'opzione della duplicazione viene messa da parte, e si preferisce un' analisi diretta in loco adoperando dei programmi appositi di ricerca e sfruttando key-word che permettano un'adeguata selezione dei file da sondare. Merita un piccolo discorso a parte il caso in cui oggetto dell'indagine (e dell'eventuale sequestro) sia un'e-mail. La procedura che si adotta è la stessa che per i siti internet con l'accortezza che il sequestro avviene presso i server del gestore che offre il servizio di posta elettronica (detto Provider). Reperire i file e i log non comporta neanche particolari difficoltà, essendo facilmente individuabili attraverso il nome utilizzato dall'utente per iscriversi al servizio o una stringa numerica identificativa. Unico problema che potrebbe sorgere è riguardo l'utilizzo di mail criptate, che dovranno essere estratte "*sic et simpliciter*", certificate e poi decriptate in un secondo momento attraverso gli appositi software.

2.1.6 *La ricerca delle fonti di prova c.d. "atipiche" e gli accessi con credenziali identificative altrui*

La ricerca delle prove informatiche non si ferma esclusivamente ai supporti fisici, infatti l'analisi affrontata finora si potrebbe definire la ricerca delle fonti tipiche delle prove informatiche. Una volta i giuristi e gli organi inquirenti facevano fatica a distinguere il supporto fisico di un dispositivo informatico (ossia l'hardware) da quello che vi era contenuto dentro (software, file, programmi applicativi ecc.), essendo più facile lavorare su qualcosa di concreto ed essendo più semplicistico discutere e ragionare solo sul sequestro di un qualcosa di materiale come un PC che anche su qualcosa di virtuale come file, dati e ecc. Un esempio eclatante di questa confusione giurisprudenziale fu il caso di una sentenza del tribunale di Savona del 17 gennaio del 2004 che assolveva con formula piena un soggetto imputato del reato di duplicazione abusiva di software (art. 171-bis legge sul diritto d'autore), in quanto l'indagine svolta appariva assolutamente lacunosa, non essendo stata effettuata né la duplicazione dei supporti di memorizzazione dei PC, né un sequestro di quest'ultimi. Quindi ad oggi il sequestro e il successivo esame di tutto ciò che è all'interno di un qualsiasi elaboratore elettronico può essere considerata un' attività tipica.

Tuttavia entrando in gioco nuove tecnologie con l'avanzare del tempo si riscontrano altri problemi, legati sempre all'individuazione e al sequestro delle fonti atipiche delle prove informatiche. Si pensi a tutto ciò che sta nel "*world wide web*" ossia il mondo, o meglio la rete, telematica ormai immanente e indispensabile per la vita di tutti i giorni. Le possibilità di archiviazione di dati e informazioni sull'internet è ormai frequentissima, basti pensare ai diversi servizi di posta elettronica o ai sistemi Cloud che permettono di caricare file di ogni tipo in una sorta di cassetta di sicurezza virtuale. Inizialmente l'utenza era scoraggiato dal massiccio utilizzo di questi strumenti, ma rafforzandone la sicurezza e l'efficienza i fornitori hanno fatto si che questa tecnologia prendesse sempre più piede essendo effettivamente comoda (non è più necessario portare il proprio laptop in giro, ma da un qualsiasi dispositivo che ha una linea internet e conoscendo le proprie credenziali è possibile accedere ai propri archivi, servizi e ecc.). Naturalmente ciò non ha fatto che complicare la vita dei giuristi, andando a

rivoluzionare indirettamente quelle che erano le precedenti definizioni di domicilio telematico e domicilio informatico (scindendo finalmente le due cose), e come poteva avvenire un accesso a quest'ultimo attraverso l'inserimento di credenziali. Questi argomenti , insieme a quello della ricerca di particolari elementi di prova, sono strettamente correlati per due ragioni. La prima è che appurato che oggi la maggior parte delle prove informatiche atipiche si trova non fisicamente sul "terminale hardware", ma su piattaforme on-line, con i dovuti adeguamenti del caso, è bene capire chi, come e quando si può accedere alle suddette piattaforme, poiché se vi è stato un accesso irregolare, potrebbero essere state apportate modifiche da soggetti esterni che comprometterebbero l'affidabilità del materiale ritrovato, nonché di conseguenza la sussistenza degli estremi di possibili reati. La seconda ragione se vogliamo è specularmente collegata alla prima. Ancor prima di effettuare un'indagine su possibili fonti di prova on-line, bisogna indagare sulla tipologia di software sulla quale quest'ultime sono presenti e come è possibile reperirle senza intaccarle e/o modificarle, al pari delle prove informatiche su dispositivi hardware.

L'uso di credenziali di identificazione in rete è una questione altamente spinosa su cui già si era espressa in passato la Suprema Corte di Cassazione che arrivava a configurare il reato di sostituzione di persona, laddove si creava un account di posta elettronica usando un nome altrui e fingendosi tale persona[50]. Nella questione che trattiamo però il caso è leggermente diverso per il fatto che non viene creato un account falso, ma vengono usati i dati identificativi originali di un altro soggetto. Di fatti trova più attinenza un'altra sentenza della Corte di Cassazione, posteriore a quella citata prima, che tratta invece il caso di violazione, sottrazione e soppressione di posta elettronica (che aveva equiparato appunto la corrispondenza all'E-mail)[51]. La sentenza stabiliva che «*tale corrispondenza può essere qualificata come "chiusa" solo nei confronti dei soggetti che non siano legittimati all'accesso ai sistemi informatici di invio o di ricezione dei singoli messaggi. Infatti, diversamente da quanto avviene per la corrispondenza cartacea, di regola accessibile solo al destinatario, è appunto la legittimazione all'uso del sistema informatico o telematico che abilita alla conoscenza delle*

[50] Cass. Pen. Sez. V, Sent. n. 46674 del 14 dicembre 2007.
[51] Cass. Pen. Sez. V, Sent. n. 47096 del 14 dicembre 2009.

informazioni in esso custodite. […] Sicché tale legittimazione può dipendere non solo dalla proprietà, ma soprattutto dalle norme che regolano l'uso degli impianti. E quando in particolare il sistema telematico sia protetto da una password, deve ritenersi che la corrispondenza in esso custodita sia lecitamente conoscibile da parte di tutti coloro che legittimamente dispongano della chiave informatica di accesso. Anche quando la legittimazione all'accesso sia condizionata, l'eventuale violazione di tali condizioni può rilevare sotto altri profili, ma non può valere a qualificare la corrispondenza come "chiusa" anche nei confronti di chi sin dall'origine abbia un ordinario titolo di accesso. […] Secondo le prescrizioni del provvedimento del Garante per la protezione dei dati personali n. 13 dell'1 marzo 2007, i dirigenti dell'azienda accedono legittimamente ai computer in dotazione ai propri dipendenti, quando delle condizioni di tale accesso sia stata loro data piena informazione»[52]. Da alcuni passaggi della sentenza possiamo evincere molti aspetti che sono alla base delle piattaforme on-line. Solitamente accedere a quest'ultime e come accedere a un sistema di posta elettronico chiuso, bisogna inserire un nome utente/ID e poi una password o un codice pin. Solitamente queste informazioni sono riservate unicamente al possessore dell'account on-line, che lo ha creato in maniera gratuita o pagando a seconda del servizio richiesto. Ma, come specificato anche dalla sentenza, in ambienti lavorativi o di studio può capitare che ad uno stesso sistema possano accedere più soggetti essendo a conoscenza delle credenziali adeguate. Anche se questa sentenza col tempo non ha avuto molto seguito, forse dovuta al fatto che con gli anni determinate dinamiche e procedimenti di accesso sono cambiati (la sentenza prende a riferimento l'accesso unicamente ad un sistema di posta elettronica e non tiene conto della possibilità odierna di poter accedere ad un sistema anche da remoto o, nel caso di piattaforme on-line, da altri dispositivi anche di natura differente dal PC, come smartphone, tablet e ecc.), ciò non toglie che tuttavia è stata formante per quegli anni ed ha chiarificato diversi aspetti che in passato creavano confusione (come la possibilità di accessi multipli ad uno stesso dispositivo e la conoscenza non univoca delle credenziali di accesso).

[52] Cass. Pen. Sez. V, Sent. n. 47096 del 14 dicembre 2009.

Infine, prima di passare alla trattazione di quali sono i sistemi attuali di archiviazione on-line, per dovere di completezza è bene parlare di una sentenza strettamente collegata a questo tema, riguardo l'utilizzo di una linea internet e la possibilità di accedervi. Si è visto che in un'indagine informatica, dove il reato si è consumato all'interno o attraverso il *world wide web*, è essenziale individuare, tramite i provider e i gestori di servizi, dove e a quale linea internet il soggetto agente si è collegato per compiere il fatto. All'interno della sentenza in esame veniva sancito che «*pur a fronte di una ricostruzione dibattimentale dimostrante il rapporto di conoscenza e di amicizia che intercorreva tra l'imputato e la persona offesa, poiché con un collegamento ADSL Wi-fi senza protezione chiunque può utilizzare un computer per mandare messaggi in Internet aventi IP riconducibili alla medesima connessione, non può dirsi raggiunta la prova, oltre ogni ragionevole dubbio, di un invio da parte dell'imputato in assenza dell'analisi del computer da lui utilizzato*»[53]. Ciò che d'importante possiamo desumere da questo estratto, similmente a quanto detto anche nella sentenza precedente, è che in riferimento al collegamento ad una linea internet, anche qui servono delle credenziali di accesso per poter usufruire del servizio. Quindi, normalmente, se è solo uno il soggetto a conoscenza di tali informazioni, per logica può essere solo quella persona ad aver potuto usufruire del servizio ed essere collegata a determinati eventi. Ma la realtà dei fatti è ben diversa, visto che questo discorso può valere semmai per le connessioni ADSL private, dato che nei luoghi di lavoro e di ritrovo le connessioni sono pubbliche, ossia vengono fornite liberamente le credenziali di accesso o addirittura non vi è neanche bisogno di inserirle. La sentenza poi dimostra come anche nel caso delle connessioni private non si ha mai la certezza assoluta che dietro un determinato IP vi sia sempre la stessa persona, sicché anche in questo caso non può essere dato per scontato che dietro ad un determinato fatto criminoso vi sia sempre lo stesso soggetto che ha stretto il contratto di rete o che solitamente utilizza la linea. Ciò in definitiva rimanda ad una maggiore accortezza degli inquirenti verso indagini meno affrettate, ma volte a controlli preventivi sulle credenziali di accesso della linea internet, del terminale fisico, ed infine delle piattaforme on-line.

[53] Trib. di Roma Sez. V, Sent. n. 22205 del 20 novembre 2009.

2.1.7 *La nuova concezione dell'uso delle credenziali e dei dati personali in rete e i sistemi Cloud*

Come anticipato poco sopra, l'esistenza dei sistemi Cloud, dei "*Social Network*" e di alcuni siti internet ha un po' rivoluzionato ciò che viene stabilito nella sentenza appena citata, per il semplice fatto che ormai non servono più le credenziali di accesso del supporto fisico per effettuare una violazione o un furto di identità o e-mail, bastando le credenziali virtuali. Per rendere ulteriormente chiaro questo passaggio bisogna tener presente che i terminali di accesso non sono più solo (o unicamente fisici), ma perlopiù sono telematici e stanno nel "*www*", facilitandone quindi l'utilizzo con qualsiasi dispositivo informatico collegato ad una linea internet. Quindi per certi versi la giurisprudenza dovrebbe aggiornarsi, ma riflettendo su quello che si ha di fronte neanche più di tanto, bastando a risolvere il problema un'ulteriore interpretazione estensiva, come lo era stato in precedenza per l'equiparazione della posta elettronica alla corrispondenza ordinaria. In questo caso si dovrebbe equiparare violazione di un terminale fisico (come un PC, uno smartphone, un tablet) ad un terminale On-line (Gmail, Dropbox, Facebook), essendo in sostanza l'azione pressoché la stessa solo che una avviene nel mondo reale e l'altra nel mondo virtuale (attraverso procedure di cracking e hacking o molto più semplicemente impossessandosi materialmente delle credenziali on-line e poi utilizzandole sui propri dispositivi in un secondo momento). A questo punto sorge spontanea la domanda: come può un inquirente durante un' indagine capire se vi è stata un'effettiva violazione? E come può reperire fonti di prova dai sistemi Cloud, soprattutto ora che sono più scrupolosi sulle normative, trattandosi spesso dati molto sensibili, oppure essendo i server non in territorio italiano? A questi interrogativi si può rispondere piuttosto agevolmente. Questi servizi offrono un sistema di certificazione strutturato proprio per cercare di capire se vi siano delle violazioni. Quando infatti si accede alla piattaforma da un dispositivo diverso (cosa piuttosto agevole da individuare per i gestori dei servizi vedendo che l'IP utilizzato dall'utente è diverso dal solito o non è tra quelli registrati), viene inviata una notifica all'email dell'utente usata per registrarsi oppure (nel caso di servizi mail appunto) viene inviato un sms sul

telefono cellulare o sullo smartphone. Questo sistema è molto celere e fa sì che in tempo reale si possa provvedere alla violazione che si sta subendo senza appunto richiedere l'aiuto dell'autorità della polizia postale e delle comunicazioni. Ciò non toglie che, vuoi per una distrazione dell'utente vuoi per un malfunzionamento del sistema Cloud, il malvivente potrebbe comunque riuscire nel suo intento di infiltrazione o furto di dati personali non essendo stato bloccato tempestivamente dai gestori. In tal caso può essere d'aiuto per l'indagine del forenser individuare innanzi tutto da dove è stata effettuata la violazione. Scoprire ciò mettendosi in contatto con i gestori dei servizi Cloud è abbastanza semplice: in primis perché per questa tipologia di servizi on-line è ormai lo standard dotarsi di un programma GPS, che permettono senza troppi problemi di circoscrivere dove avvengono fisicamente i vari accessi. Perciò in caso di accesso anomalo tempestivamente si può triangolare la posizione del soggetto che ha effettuato l'effrazione, o sarebbe più corretto dire il luogo in cui quest'ultimo l'ha compiuta. In secundis si può risalire anche al dispositivo utilizzato dal reo attraverso l'indirizzo IP (che come dicevamo pocanzi vengono sempre controllati dai sistemi Cloud). Di solito è proprio grazie agli IP che funzionano i sistemi GPS, essendo questi "*indirizzi telematici*" molto precisi e accurati. Conoscendo questo dato infatti (che in sé e per sé costituisce una stringa numerica) è possibile risalire a qualsiasi dispositivo (c.d. "*host*") collegato ad una linea informatica. Un'eccezione è rappresentata da sistemi Cloud "*client*"[54] che non lasciano nessuna traccia di memorizzazione sul dispositivo utilizzato, rendendo molto difficile se non impossibile il reperimento di informazioni. Per dovere di completezza tuttavia è necessario anche segnalare la possibilità che chi abbia commesso la violazione si sia servito di dispositivi pubblici o aperti al pubblico (i PC di un internet-cafè o di un'università) o ancora rubati. In tal caso è chiaro che risalire al colpevole sarà più complesso, ma comunque sia si avrà sempre un buon punto di partenza come un luogo geografico specifico da cui far partire le indagini.

La possibilità di effettuare un sequestro del sistema Cloud attraverso richiesta del p.m. non è da escludere nel caso i server sia fisicamente collocati all'interno dello stato, in tal caso la procedura che ne seguirebbe sarebbe grosso modo la stessa per

[54] S. Aterno e M. Mattiucci, *Cloud Forensics e nuove frontiere delle indagini informatiche nel processo penale*, in *Archivio Penale,* fascicolo 3, 2013, pag. 865–878.

i server e i siti internet per ciò che riguarda il reperimento di log, con particolare attenzione a cosa si va a sequestrare e al metodo di custodia dei dati, non essendo possibile "*cristallizzare*" la situazione *sic et stantibus* come nei server generici. Tuttavia un ostacolo che potrebbe incontrare l'inquirente è il caso in cui i server del sistema Cloud siano situati in territorio straniero. Se il gestore del servizio si dimostra poco collaborativo con le autorità l'unico modo per procedere è attraverso rogatoria internazionale o intercettazioni telematico-informatiche. Per fortuna essendoci di solito dietro quest'ultimi compagnie con determinati codici etici o che comunque tengono alla loro immagine spesso si dimostrano cooperativi con le forze dell'ordine (ciò non toglie però che esistano compagnie estere che sono di tutt'altro avviso, un esempio è dato dall'impresa Apple che non è autorizzata a fornire dati dal suo sistema iCloud se non dietro permesso dell'autorità garante americana). Finora poi si è analizzata la situazione come se ci trovassimo di fronte ad un Cloud essenzialmente privato. Qualora il Cloud fosse pubblico ci sarebbe anche la problematica dell'ingente mole di dati corrispondente al numero degli utenti, per non parlare poi di quei gestori che criptano i file dei propri iscritti, rendendo difficoltosa non solo un'eventuale intercettazione, ma anche nel caso in cui si ottenessero i dati per vie pacifiche, questi verrebbero comunque consegnati criptati.

Di fatto quindi il metodo più efficace per ottenere informazioni e prove in un'indagine che coinvolge un sistema Cloud è quello di cogliere in flagranza di reato il colpevole oppure durante l'ispezione reperire il dispositivo informatico acceso collegato ancora al servizio. Per concludere, al fine di diminuire i rischi di un'eventuale infiltrazione non voluta da parte de esterni, sta diventando prassi dei sistemi Cloud chiedere un doppio accesso (ad esempio tramite numero cellulare e credenziali on-line), in maniera tale da evitare a monte il problema delle violazione e rendere ulteriormente più sicuro il sistema.

2.1.8 *Le intercettazioni informatico-telematiche*

L'ultima questione da affrontare nel campo della ricerca delle prove informatiche riguarda l'effettuazione e il reperimento delle intercettazioni telematiche, e la loro differenza con le classiche intercettazioni telefoniche e

ambientali. Innanzi tutto un'intercettazione di tipo telematica-informatica è sempre una captazione di un flusso comunicativo tra due e più persone, con l'eccezione che non sempre la comunicazione avviene per forma verbale, ma attraverso messaggi (talvolta anche vocali) di chat. L'intercettazione di comunicazioni informatiche e telematiche sono previste dall'art. 266 bis c.p.p. (legge 547/1993), prevista per i reati indicati all'art. 266 c.p.p., quelli commessi mediante mezzi informatici o telematici, e per il reato previsto dall'art. 600 ter c.p., (legge 269/98). Il pubblico ministero (ex art. 267 c.p.p.) richiede al GIP l'autorizzazione a disporre le operazioni, che viene concessa con decreto motivato se vi sono gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini. L'autorizzazione è di 15 giorni, con la possibilità di proroga da parte del GIP con decreto motivato per i successivi 15 giorni, non necessariamente contigui ai primi, se sussistono determinate esigenze investigative. Questo metodo di indagine viene utilizzato non solo per i reati informatici, ma per qualsiasi reato in cui sono coinvolti mezzi telematici. Inutile sprecare parole su quanto questo metodo di indagine sia proficuo, forse ancor più di un'intercettazione classica vista la modernità dei tempi e la preferenza del crimine organizzato nel scegliere metodi di comunicazioni sempre più sofisticati, e sia soggetto a costante innovazione proprio per far fronte all'ingegno degli indagati nell'evitare di essere intercettati (utilizzando per esempio canali criptati o protocolli sicuri che non permettono un acquisizione in tempo reale).

Se da una parte quindi il paragone con le intercettazioni telefoniche è concettualmente semplice, dal punto di vista pratico l'operazione differisce non poco essendo quella telematica-informatica molto più complessa. Per effettuare un'intercettazione ottimale di questo tipo è necessario collegarsi o alla stazione telefonica o al sistema che trasmette le comunicazioni. In seguito bisogna far attenzione alla tipologia di linea di cui usufruiscono gli indagati: questo fattore è importante a determinare la quantità di dati che devono essere intercettati (una linea domestica che sfrutta unicamente un modem sarà sempre più facile da gestire rispetto a chi invece si appoggia ad una ADSL su banda larga dove invece passano molti più dati). I metodi concreti per effettuare le intercettazione sono vari e piuttosto eterogenei (tal per cui verranno esposti con più chiarezza nel prossimo paragrafo), e vengono scelti a seconda dei mezzi o della situazione che il

forenser ha davanti, infatti secondo l'art. 268 comma 3 bis c.p.p. è possibile effettuare le intercettazioni anche «*avvalendosi di impianti privati indipendentemente da ragioni di urgenza e di insufficienza degli impianti della Procura della Repubblica*».

Infine si presenta la possibilità sia di effettuare le intercettazioni di questo tipo però con finalità preventive però solo per reati di un certo tipo, come quelli con finalità di terrorismo e della criminalità organizzata (secondo il combinato disposto sia dalla legge del 23 Dicembre n. 547/1993 e la legge 18 Ottobre n.374/2001), sia direttamente presso i fornitori dei servizi di chat (ossia i provider) in maniera tale da poter risalire direttamente alle persone dietro le conversazioni attraverso i loro IP. Naturalmente anche in questo caso il provider deve risiedere in territorio italiano, altrimenti valgono le regole e le procedure già esposte nel caso di server collocati all'estero[55].

Attualmente è possibile ravvisare delle valide alternative nel modus operandi degli inquirenti nell'effettuare delle intercettazioni. Una tecnica abbastanza diffusa è quella dello "*Sniffing*", che consiste nel cercare di inserirsi nel flusso di comunicazione tra il soggetto sospettato e il punto di connessione alla linea internet a cui quest'ultimo si allaccia . In questo modo vengono captati qualsiasi tipo di dati dalle mail ai file audio e via discorrendo, bypassando ogni limite che potrebbe nascere dall'inserimento di credenziali. Unico problema, comune a qualsiasi intercettazione telematica, si presenta nel caso in cui vengano utilizzati chat criptate oppure protocolli sicuri. Qualora ciò accada è possibile comunque effettuare l' intercettazione, ma si acquisiranno solo dati criptati che dovranno essere successivamente decifrati con non poca difficoltà e spreco di tempo. Quest' operazione può essere semplificata nel caso in cui si sia a conoscenza dei certificati su cui si basano i protocolli. Oltretutto statisticamente questo tipo di tecnologia, benché sicura, viene poco utilizzata per gli elevati costi («*il traffico criptato al giorno d'oggi rappresenta meno del 5% del traffico complessivo in*

[55] G. Conso, V. Grevi, M. Bargis, *Compendio di procedura penale*, CEDAM, 2014.

rete […] e viene impiegato per comunicazioni riservate su servizi bancari, pagamenti on-line, fornitura di dati personali»[56]).

Essendo spesso le intercettazioni telematiche condotte di pari passo con quelle telefoniche si preferisce e si è soliti utilizzare uno strumento più classico e datato come il "*Telemonitor*", o comunque mezzi meno obsoleti che svolgono la stessa funzione, in maniera tale da poter captare sia dal numero di cellulare o di telefono, sia dall'indirizzo IP utilizzato dall'utente con la sua linea. Ancora tra le tecniche in questo settore annoverabili vi è la duplicazione delle caselle di posta elettronica utilizzate dall'indagato. «*Questa è una forma particolare di intercettazione telematica e, pertanto, è sottoposta al nulla osta del GIP, il quale emetterà un apposito decreto, valido per la durata di 15 giorni con la possibilità di proroga. Tale attività permetterà l'acquisizione della posta in giacenza, in arrivo e trasmessa dal giorno di inizio delle operazion*i»[57].

In conclusione meritano menzione due sistemi di intercettazione di recente innovazione: il "*Keylogging*" e l'utilizzo di Trojan. Con il primo termine si vuole intendere un'intercettazione selettiva su più parametri che permette attraverso un programma di captare quelle comunicazioni che utilizzano determinate parole chiave che vengono digitate. Il vantaggio di questo metodo è quello di permettere indagini mirate così da evitare lunghe ed estenuanti ricerche oppure di entrare in altri ambiti non d'interesse, inoltre funziona anche se il dispositivo non è inizialmente collegato alla linea internet. Con il secondo termine invece si intendono i già citati virus Trojan, modificati appositamente per compiere le operazioni di intercettazione. Il loro utilizzo, da un punto di vista pratico, e pressoché simile a quando vengono usati nelle indagini per i sistemi Cloud. Tuttavia solitamente si sconsiglia l'utilizzo di questo strumento per diverse ragioni. Innanzi tutto è sempre presente la difficoltà di trovare un modo per infettare il computer, sia che si cerchi un approccio fisico (collegando una pennetta USB con il virus al dispositivo ad esempio) dovendosi presentare un'occasione opportuna per poterlo fare, sia che si tenti di farlo attraverso procedure ed escamotage on-line, dovendo cercare di aggirare eventuali anti-virus

[56] G. Amato, V. Destito, G. Dezzani, C. Santoriello, *Op. Cit*., pag.149.
[57] M. Delle Donne, *Tecniche di indagine della Polizia Postale nell'ambito dei reati informatici e nella pedo-pornografia on-line*, in *Diritto&Diritti*, 2004.

e firewall. In aggiunta questa tipologia di virus una volta installato crea possibilità di modificare i dati o le impostazioni di base del dispositivo. Ciò significa (come verrà spiegato più approfonditamente nel prossimo paragrafo) che essendo altamente soggetti a modifiche i dati potrebbero non soddisfare i requisiti minimi di acquisizione e garanzia delle prove informatiche per poter essere considerati effettivamente validi in un processo penale, compromettendo quindi l'intera indagine. Ragion per cui si sconsiglia solitamente nelle linee guida di adottare questa via se non in casi estremi o sui generis.

2.2 *I nuovi metodi di investigazione, le prassi e le nuove tecnologie*

Il progresso con cui la tecnologia viaggia è davvero sorprendente (un recente studio ha dimostrato che ogni sei mesi i sistemi computerizzati si evolvono come se in realtà fossero passati due anni). Altrettanto sorprendente è vedere come tante innovazioni riguardino il settore investigativo, soprattutto in quei campi che abbiamo appena trattato nel paragrafo precedente. L'innovazione, sia dal punto di vista tecnologico che da quello del diritto, è alla base della computer forensics. Non deve meravigliare dunque che determinati metodi e/o prassi vengano riviste, sostituite o reinventate anche in periodi di tempo relativamente brevi. Iniziando dai dispositivi hardware classici, come PC e smartphone, si è visto che la prassi consigliata dalle "*best practice*" è quella di utilizzare "*block writer"* o, ancora meglio, dei duplicatori forensi. Ciò non toglie tuttavia che la maggior parte dei forenser, esperti o con particolari abilità tecniche, si dota per prima cosa di duplicatori e block witer di varia natura a seconda del dispositivo che dovrà esaminare (un po' come un manutentore che si porta dietro diversi tipi di cacciavite a seconda della riparazione). In secondo luogo un operatore che ha una certa dimestichezza con i programmi, spesso crea software *sui generis* modellati a suo piacimento a seconda della circostanza. Questo è possibile grazie a determinati programmi di computer-informatic forensics che, essendo Open Source (e quindi modificabili dall'utente), permettono un'alta personalizzazione dei propri strumenti del mestiere. La combinazione di nuovi hardware e software permette, quindi, di aprire a nuove tecniche investigative, che possono essere più efficaci delle prassi standard già consolidate nelle linee guida.

Tuttavia, sebbene l'utilizzo di questi nuovi *tools* possa portare a risultati decisamente più efficaci, rimane sempre il problema di vedere se questi siano conformi alle linee guida e agli standard internazionali, poiché in caso contrario le prove raccolte non potrebbero essere considerate valide per formare la decisione del giudice[58]. Vediamo ora alcune delle tecniche di più recente ideazione utilizzate nelle indagini informatiche.

2.2.1 *La tecnica del Clustering*

In un'indagine che coinvolga sistemi informatici è usuale che spesso si rilevi che diversi dati, all'interno del dispositivo oggetto di esame, siano stati cancellati. Ciò può avvenire per diverse regioni: un errore degli inquirenti, programmi di pulizia che operano in maniera periodica o lo stesso proprietario del terminale che prima di consegnarlo ha eliminato materiale che poteva essere compromettente. In tal caso viene in soccorso una recente tecnica di analisi, di cui ormai si fa largo uso per la sua utilità, ossia il "*Clustering*". Ogni dato, nel momento in cui viene memorizzato, viene scomposto in varie parti (c.d. Cluster) e salvato in determinate aree della memoria di massa c.d. "*directory*" (questo processo fa si che vi sia una certa celerità nell'elaborare il dato nel momento in cui viene "*richiamato*"). Quando il dato viene cancellato grazie al sistema dei cluster lascia delle tracce, ed è così possibile a volte ricostruire in parte i file eliminati. Questo metodo di indagine è basato sull'utilizzo di diversi algoritmi, a seconda dei casi, che effettuano la ricerca e il recupero dei diversi file eliminati. Il ruolo di questi algoritmi è fondamentale se si pensa che già in un computer di per sé vi sono una moltitudine di dati memorizzati. Andare a ricercare ed analizzare anche i dati, parzialmente o no, cancellati si rivelerebbe un'impresa senza fine se per l'appunto non ci fosse un sistema in grado di preselezionarli e smistarli. In pratica, quindi, l'algoritmo svolge un ruolo simile a quello di un analista di *data-meaning*, che, non potendo conoscere il contenuto di tutti i file processati, tramite cluster comuni raggruppa i file in macro sezioni, che poi verranno selezionati successivamente dagli inquirenti. Il fatto che ci si affidi ad un programma che

[58] L. Filippi, *Il rilevamento del "tracciato axe": una nuova denominazione per una vecchia tecnica d'indagine*, in *Giurisprudenza italiana*, 1999.

smisti le informazioni di certo semplifica ed accelera il corso delle indagini. Ma poiché quest'ultimo, al contrario di una persona cosciente, agisce in maniera meccanica ed automatica nella ricerca, si rende doveroso porre particolare attenzione alle impostazioni di base che si immettono prima di effettuare l'analisi. Ad oggi esistono in tutto sei tipi differenti di algoritmo (K-means, K-medoids, Single link, complete link, Average Link, CSPA)[59], ognuno con parametri differenti a seconda della tipologia di cluster da ricercare. Una volta scelto l'algoritmo da usare, prima di iniziare il caricamento dei diversi documenti, vengono preliminarmente indicate ed escluse le "*common words*", ossia articoli, pronomi, congiunzioni, numeri e altre parole frequenti derivate che potrebbero bloccare il programma e generare confusione o risultati errati. Una volta avviata, la ricerca dei cluster raccoglierà tutti i file che presentano, o presentavano, un certo indice di frequenza dei termini c.d. TF (*term frequency*) ed una determinata distanza tra un termine e l'altro ("*distanza di Levenshtein*"). La correlazione dei diversi documenti avviene successivamente, in base ai vari indici TF rilevati e le loro distanze. Tutti i file che presentano risultati di analisi simili vengono raggruppati, in questo modo i cluster vengono ricompattati, come quando erano memorizzati nelle directory, ed è così che i documenti vengono ricostruiti. A questo punto, sui risultati conseguiti, viene creato un database con diverse voci correlate in base al tempo e all'oggetto del documento. Spetterà poi all'investigatore, seguendo le indagini fino a quel momento condotte, scegliere quali file estrarre. Molti programmi, infine, permettono, al momento della creazione dell'archivio informatico, di garantire già la validità dei dati recuperati attraverso certificazione, in maniera tale che all'occorrenza non sia necessario effettuare ulteriori operazioni e le prove possono essere valutate ed acquisite facilmente all'interno del processo.

È facile comprendere come tutto ciò sia estremamente adatto in quei casi in cui vengono attivati, o si attivano automaticamente, programmi di eliminazione o pulizia dei dati in quei sistemi dove è possibile pre-impostare questa funzione alla loro accensione o spegnimento. Anche se dalla ricerca uscissero fuori solo

[59] J. Shankar Babu, K. Sumathi, *"An Approach to Improve Computer Forensic Analysis via Document Clustering Algorithms",* in *International Journal of Innovative Research in Computer and Communication Engineering*, IJIRCEE, Vol. 2, Special Issue 4, settembre 2014.

informazioni parziali, quest'ultime possono avere una certa rilevanza. Questo perché da esse è possibile, attraverso rielaborazioni, ricostruire l'intero file oppure estrapolare tracce che possono far sorgere punti di svolta nelle indagini. Tuttavia questo strumento di indagine presenta dei limiti. Il più grande di tutti è decisamente il fattore tempo. Come già detto, la mole di dati che vengono sottoposti al procedimento può essere di ingente entità e ciò significa che per produrre risultati concreti potrebbe servire un intero mese se non di più. Altra problematica è quella della "*Scalability*", una sorta di conflitto nella ricerca che può avvenire quando, per velocizzare o ottimizzare il lavoro di analisi, vengono utilizzati più algoritmi combinati tra di loro. Infine l'utilizzo di questo è molto complesso, essendo più idoneo far svolgere questo compito ad un vero e proprio ingegnere informatico, più che ad un forenser. Le competenze di base richieste per gestire gli algoritmi e l'intero processo sono piuttosto elevate e ciò rende il lavoro per nulla facile. Lasciare quindi quest'incarico a mani inesperte potrebbe compromettere l'intera operazione, e dati i tempi di elaborazione si rivelerebbe un inutile spreco di risorse [60].

Questa tecnica è strettamente collegata con un altro metodo particolare di indagine per reperire indizi e/o prove è quella di analizzare i "*metadati*"[61]. Con tale definizione si intendono quelle informazioni circostanziali che ruotano attorno al file. A seconda della tipologia è possibile conoscere se e quando un file è stato creato, modificato o quando è stato aperto l'ultima volta e conoscere anche quale dispositivo proviene o da chi è stato inviato e/o creato. Talvolta queste informazioni si dimostrano ancora più utili dello stesso file, poiché possono contribuire a creare una "*time-line*" degli eventi o scoprire se vi siano state delle manomissioni sugli elementi di prova rilevati.

[60] I. Riadi, *Log Analysis Techniques using Clustering in Network Forensics*, in *International Journal of Computer Science and Information Security,* IJCSIS, Vol. 10, n.7, luglio 2012 .
[61] G. Amato, V. Destito, G. Dezzani, C. Santoriello *, Op. Cit*., pag.186.

2.2.2. *Le tecniche specifiche per i sistemi Cloud*

Nell'ambito dei sistemi Cloud oppure dei siti WEB si è constatato che la più grande difficoltà, quando si compiono indagini che li coinvolgano, è quella di trovare tracce utili che colleghino il dispositivo dell'indagato alle suddette piattaforme virtuali. Recentemente si sta diffondendo il fenomeno della "*Cloud community*"[62] che, sia per via lecite sia molto più spesso per vie illecite, fa si che i documenti o file che servono agli utenti vengano scomposti e conservati dai componenti della community, e vengano ricomposti solo quando qualcuno ne fa richiesta. In questo modo non solo il file tecnicamente non esiste, o meglio non è in grado di essere classificato come lesivo o oggetto pertinente al reato, ma è anche estremamente difficile da recuperare essendo sparso in diversi server in tutto il mondo (si prenda ad esempio un' immagine digitale dal contenuto pedopornografico i cui Byte vengano divisi tra gli utenti e che l'immagine venga ricomposta solo nel momento in cui vi sia un cliente disposto ad acquistare l'immagine). Per far fronte a questo problema le forze dell'ordine hanno escogitato due soluzioni di recente inventiva. La prima è una sorta di infiltrazione sotto copertura riadattata per i sistemi telematici-informatici. Un agente attraverso un dispositivo privato e con credenziali false viene introdotto o cerca di introdursi in queste community, che molto spesso risiedono nel WEB sommerso (anche detto "*Deep-WEB*", ossia un'area nascosta dell'internet raggiungibile solo con appositi motori di ricerca come Tor). In questo modo sarà possibile mettersi in contatto con gli altri utenti e cercare di reperire informazioni sulle altrui identità o comunque sulle fonti del materiale compromettente. Tuttavia questo sistema per lo più riesce a reperire solo materiale indiziante che difficilmente potrebbero servire a incriminare in maniere definitiva un indagato. Ragion per cui veniamo al secondo espediente utilizzato dagli investigatori. Si è già detto che l'ipotesi migliore in una indagine che coinvolga sistemi Cloud o siti WEB è quella della flagranza di reato, e quindi quella di sorprendere il sospettato mentre visiona o scarica materiale criminoso oppure mentre utilizza siti e/o Cloud per farlo. In questo caso l' utilizzo dei mezzi informatici per compiere il reato in un certo senso facilità la possibilità di cogliere sul fatto il soggetto, questo perché

[62] S. Aterno e M. Mattiucci*, Op. Cit*., pag. 872.

attraverso dei sistemi di controllo remoto o dei virus "*Trojan*" è possibile seguire i movimenti virtuali dell'indagato o addirittura vedere attraverso il proprio monitor le sue operazioni come se si fosse fisicamente con lui acquisendo le immagini dello schermo. Naturalmente questo metodo non è esente da difetti, infatti il sistema di controllo remoto deve essere in qualche modo collegato o connesso al dispositivo che potrebbe essere utilizzato per compiere il reato, mentre i virus Trojan devono attecchire al sistema operativo, quindi non solo si deve cercare in qualche modo di infettare il dispositivo sperando che il suo anti-virus non lo rilevi, ma oltretutto esso deve permanere e non essere cancellato finché non si hanno elementi per intervenire. Infine entrambi i sistemi sono metodi altamente intrusivi che devono essere utilizzati con la massima accortezza, in casi di vera emergenza quando nessun altro mezzo investigativo ha portato svolte significative nelle indagini, poiché si potrebbero violare determinati diritti costituzionalizzati importanti come il diritto alla riservatezza o alla privacy. Sicché è deducibile che il compenso di valori che viene effettuato quando si decide di utilizzare questo tipo di mezzo di ricerca della prova deve essere molto ponderato, come avviene d'altronde anche per altri strumenti d'indagine decisamente invasivi come le intercettazioni sia telefoniche che informatiche.

2.2.3 *La tecnica della ricostruzione di immagini 3D*

«*Quando scattiamo una fotografia di certo non consideriamo che in quel momento oltre a catturare la scena che ci interessa, stiamo anche raccogliendo e fissando in modo indelebile un elevato numero di ulteriori informazioni, di cui l'immagine digitale è portatrice. Questi dati possono rivelarsi utili in altri contesti quali, ad esempio, quello investigativo dove, facendo uso di appositi strumenti informatici è possibile estrarre particolari a prima vista non disponibili e, sotto certe condizioni, persino ricostruire con notevole precisione la rappresentazione tridimensionale (3D) cui fa riferimento l'immagine bidimensionale di partenza*»[63]. Questa tecnica della Digital forensics lavora

[63] S. Battiato, F. Galvan, *Ricostruzione di informazioni 3d a partire da immagini bidimensionali*, in *Sicurezza e Giustizia*, 2013, pag. 38.

unicamente su i file di immagini, come i BMP, GIF, JPG/JPEG, PSD e ecc., e fondamentalmente ha due funzioni: la prima è capire se un file di natura fotografica è stato alterato e/o modificato parzialmente o totalmente, constatando la sua natura e di conseguenza la sua affidabilità come prova con relativa valutazione da parte del giudice all'interno del processo; la seconda è una ricostruzione del *locus commissi delicti* artificiale, in maniera tale da poter fare riscontri e paragoni con la zona reale in tempi differenti, ed anche esperimenti giudiziali di diversa natura per comprendere la dinamica dei fatti (l'esempio più noto di questo utilizzo fu durante il "caso Garlasco", con una ricostruzione del pavimento e di alcuni ambienti per capire se fosse possibile muoversi in essi senza sporcare di sangue le scarpe).

Questo metodo di indagine prende ispirazione e ha origine da alcuni procedimenti, utilizzati dagli studiosi di storia dell'arte, per analizzare la prospettiva e la profondità dei quadri. Nella Digital forensics l'esame è tuttavia parzialmente diverso. Come già detto si prende ad oggetto un'immagine digitale o una fotografia che ha comunque origine da un file, di conseguenza prima ancora di iniziare la ricostruzione si rende necessario acquisire determinati dati. Innanzi tutto bisogna sapere la tipologia e il modello della fotocamera che ha prodotto la foto, in seguito, in base a ciò che compare all'interno di essa, prendere nota delle proporzioni e degli spazi. Come accade poi anche con i quadri vengono individuati i punti di fuga e la prospettiva in maniera tale che la ricostruzione può essere la più precisa possibile. All'uopo solitamente, se possibile, vengono effettuati anche dei rilevamenti tecnici sul luogo reale dove stata scattata la foto, in maniera tale da diminuire il margine di errore. Ciò non toglie che, anche con queste premesse di base, si possano verificare delle difficoltà nel corso del lavoro, come ad esempio delle prospettive falsate o ingannatorie, o ancora la presenza di immagini in due dimensioni che per loro natura non possono essere proiettate. A queste problematiche si può ovviare facilmente o con dei rilevamenti tecnici o con l'utilizzo di più immagini che permettono una ricostruzione più pedissequa e precisa dell'ambiente. I *forenser* per questo lavoro di solito si forniscono di appositi software di analisi (il più diffuso in commercio è "*AmpedFIVE*"[64]), anche

[64] http://ampedsoftware.com/it/

se ad oggi sono diffusi diversi programmi on-line[65], che sebbene semplificati e non precisissimi, sono ideali per effettuare ricostruzioni immediate abbastanza accurate[66].

2.3 *L'Acquisizione e la valutazione dell'attendibilità delle prove*

Le prove informatico-digitali presentano diversi vantaggi grazie alla loro varietà e alle numerose informazioni che è possibile trarre da quest'ultime. Purtroppo però presentano anche un solo grande difetto insito nei limiti della loro natura informatica, ossia l'alta volatilità e la possibilità di essere alterati facilmente. Il nostro ordinamento non prevede leggi puntuali e precise da rispettare per il recupero della prova digitale. Basti pensare che di fatti non esistono regole specifiche sulla nullità di una *digital evidence* o sulla loro inutilizzabilità. Ciò non toglie che il nostro ordinamento prevede dei requisiti minimi introdotti nel nostro codice di procedura penale nel 2008, in linea con gli standard internazionali della documentazione RFC3227[67] e le "*best practice*"[68], per far si che questo tipo particolare di prove siano garantite e considerate valide ai fini di un processo penale fugando ogni dubbio sulla loro genuinità e attendibilità. Nelle linee guida ci si concentra soprattutto sul obiettivo da raggiungere a seconda dei casi e delle situazioni che emergono, questo fa si che l'attinenza a tali normative non sia fiscale ma sia volto totalmente al risultato finale dell'acquisizione. Qualora infatti quest'ultima presenti delle mancanze o presenti delle irregolarità, ne saranno tenute conto in fase di giudizio[69]. In sostanza quindi il lavoro del forenser non si esaurisce solo con il recupero sicuro delle tracce e degli elementi probatori, ma deve anche assicurarsi che quest'ultimi rimangano immutati fino alla loro valutazione in sede processuale e anche in

[65] https://photosynth.net/

[66] H. Farid, M. Bravo, "*Image forensic analyses that elude the human visual system*" in *SPIE Symposium on Electronic Imaging*, San Jose, CA, 2010;
S. Battiato, F. Galvan, *Op. Cit*.

[67] Sito di riferimeto http://www.rfc-base.org/rfc-3227.html*, Guidelines for evidence collection and archiving*, 2002.

[68] Documentazione NHCTU: association of chief police officers, *The good practices guide for computer based electronic evidence*, 2003,(il documento è reperibile al sito http://www.7safe.com/electronic_evidence/ACPO_-guidelines_computer_evidence.pdf).

[69] M. Daniele, *La prova digitale nel processo penale*, in *Rivista di diritto processuale* Anno LXVI (seconda serie) – n.2, 2011.

seguito ogni qual volta sia necessario analizzare o esaminare quei dati, comportando in conclusione l'uso di un'estrema delicatezza e competenza da parte di chi svolge queste operazioni, poiché ne va di mezzo l'ammissibilità della prova e di conseguenza le sorti dell'intero giudizio[70].

Per ottenere senza problemi questo obiettivo gli inquirenti, quando si trovano di fronte ad una possibile prova informatica, devono seguire pedissequamente le istruzioni della Catena di custodia (c.d. "*Chain of Custody*") indicata nel testo delle linee guida o best practice a cui si fa riferimento o che gode del maggior pregio[71]. Solitamente questa procedura prevede diverse fasi sequenziali che se adottate sistematicamente garantiscono una certa sicurezza sulla immutabilità dei file acquisiti (naturalmente la catena di custodia dovrà essere applicata sia nel caso dei reati informatici, ma anche sicuramente per tutti quei reati canonici dove sono coinvolti mezzi telematici e informatici). Inoltre è bene specificare che casomai una delle fasi fosse eseguita male o saltata, ciò comprometterebbe l'esito dell'intera catena, non essendo più affidabile l'autenticità di quei dati[72].

Altra tecnica è quella invece del "*contraddittorio tecnico*", che presenta tuttavia diverse perplessità essendoci ancora, a parere della dottrina[73], molta insicurezza su quale sia il giusto metodo con il quale instaurare il contradditorio su queste prove. Al momento le teorie possibili più praticabili e che stanno avendo seguito sono tre. La prima via prevede che il reperimento delle prove informatiche sia assoggettato alla regola dell'art. 359 c.p.p., e quindi essere considerati accertamenti tecnici ripetibili che non necessitano delle garanzie maggiori offerte dall'art. 360 c.p.p. (accertamenti non ripetibili). Indubbiamente questa scelta va a penalizzare la difesa, che non sarebbe preventivamente avvisata, né avrebbe la possibilità di far partecipare al recupero un proprio tecnico o specialista ed infine non potrebbe chiedere successivamente l'incidente probatorio. Aldilà di questa specificazione questa ipotesi si basa appunto sul postulato che sia possibile ogni volta effettuare una copia forense uguale all'originale in ogni momento

[70] A. Macrillo', *Op. Cit*.
[71] C. L. T. Brown, *Computer evidence: Collection & Preservation, Charles River media Inc*., 2006.
[72] F. Bravo*, Indagini informatiche e acquisizione della prova nel processo penale*, in *Rivista di Criminologia, Vittimologia e Sicurezza* Vol. III - n. 3; Vol. IV – n. 1 – Settembre 2009/Aprile 2010.
[73] M. Daniele, *Op. Cit.*

dell'indagine. Ciò in parte è corretto ed in parte no. È vero che la copia che si effettuerà sarà uguale all'originale, è falso dire che se si effettua la copia in un secondo momento questa sarà sempre identica a quella creata precedentemente (ancora una volta calza perfettamente l'esempio che vede la copia forense come una sorta di fotografia, infatti se fotografassimo un'oggetto, anche se quest'ultimo non è stato spostato o modificato, comunque a seconda del tempo trascorso o del momento della giornata potremmo avere due foto abbastanza diverse). Quest'ultima affermazione acquista ancora più fondamento se nell'acquisizione delle copie digitali non si fa uso degli adeguati mezzi, come un *block writer* o un certificatore forense. Infine riconoscere al difensore anche solo il preavviso sarebbe comunque una grande occasione per quest'ultimo per avere una chiara visione dei movimenti delle indagini. Anche se quest'ultimo è neofita sotto l'aspetto tecnico potrebbe comunque fare presenti successivamente eventuali irregolarità o dubbi sulle procedure di acquisizione adottate.

La seconda via prevede, al contrario, un pieno assoggettamento della prova digitale alla regola dell'art. 360 c.p.p. La parte della dottrina[74] che avvalora questa ipotesi parte da presupposti totalmente opposti a quelli del punto precedente, ritendo il fornire un maggior garantismo alla difesa indispensabile, visto che essendo le prove digitali irripetibili, il coinvolgimento sia dell'imputato che del suo difensore devono essere immediati per impedire abusi o incomprensioni nel reperimento e la custodia di questi particolari elementi di prova. Tuttavia abbracciare totalmente questo punto di vista comporta effettivamente uno squilibrio della bilancia del contradditorio a favore della difesa, che potendo usufruire dei diritti e delle garanzie dell'art. 360 c.p.p. e della peculiare volatilità dei file e dati digitali, potrebbe in questo modo ad alterare in maniera non indifferente i risultati delle indagini (anche se bisogna sottolineare che collaborazioni di questo tipo tra persona indagata e/o imputata e legale nella gran parte dei casi sfociano nel favoreggiamento personale, punito ex art. 378 c.p., se quest'ultimo non si limita a dare suggerimenti al proprio assistito, ma comunica preventivamente i controlli degli inquirenti consigliando di eliminare ogni elemento compromettente).

[74] A. Ester Ricci, *Digital evidence e irripetibilità delle operazioni acquisitive*, in *Dir. Proc. Pen.*, Giuffrè, 2010.

Infine la terza via prevede una sorta di compromesso e fusione delle due precedenti, e forse proprio per questo si ritiene che sia la scelta più adeguata. Essendo le prove informatiche una tipologia di prova *sui generis,* che può presentare caratteri eterogenei, l'approccio ideale è quello di valutare volta per volta la presenza o meno della loro irripetibilità, ed in base ad essa agire di conseguenza e regolare i rapporti tra accusa e difesa. Di certo devono però essere fornite comunque delle garanzie di base ad entrambe le parti processuali. La difesa deve avere la possibilità di poter assistere alle indagini, anche se senza preavviso, e poter contestare in dibattimento le prove informatiche raccolte precedentemente, avvalendosi anche di esperti tecnici. D'altra parte gli inquirenti devono avere la possibilità di poter effettuare le indagini non informando l'indagato in maniera tale da sorprenderlo ed evitare l'eliminazione preventiva di prove ed indizi significativi, che comunque potranno essere contestate successivamente[75].

2.3.1 *Le operazioni della Catena di Custodia*

Le operazioni della catena di custodia iniziano nel momento in cui su una scena del crimine vengono reperiti materiali d'interesse di origine telematico-informatico.

La prima fase prevede un giudizio da parte degli investigatori riguardo appunto l'attivare ed applicare i protocolli di sicurezza per gli elementi reperiti sul campo, e se vi è necessità di far intervenire l'autorità giudiziaria competente.

In secondo luogo si procede con un'adeguata documentazione fotografica del "*locus commissi delicti*" e dei reperti rinvenuti. In questo modo si ha una visione completa di quali dispositivi sono presenti e sono stati usati, e se sono accesi che programmi o siti compaiono attivi. Questo passaggio può rivelarsi particolarmente utile nel caso in cui i sistemi vengano poi abdotti dalla loro posizione d'origine attraverso il sequestro oppure vengano comunque spenti, e sia necessario fare un confronto, anche solo visivo, di ciò che risultava essere presente sul dispositivo al

[75] M. Daniele*, Op. Cit*.

momento del ritrovamento e vedere se è ancora presente. In seguito bisogna raccogliere e verbalizzare diverse informazioni circostanziali riguardo il materiale probatorio con relativa modulistica a seconda di ciò che si è rinvenuto, come ad esempio chi ha reperito la prova digitale e in quale stato. Questi dati sono essenziali per ogni successivo esame (essendo non raro che in un processo, per colpa dei tempi dilatati, determinate operazioni peritali vengano esposte nel giudizio anche dopo che è trascorso diverso tempo dal reperimento), ed è per questo che solitamente si ci sofferma in particolar modo sul luogo, sulla data e sull'orario del ritrovamento. Ancora più nello specifico si confronta di solito l'orario e il fuso orario dei dispositivi con l'orario ufficiale. Di solito tutti i file un sistema hanno indicati sia data e ora della creazione sia data e ora dell'ultima modifica, quindi se ne deduce facilmente che se eventualmente ora di sistema e UTC non corrispondono sarà necessario prendere atto della differenza del lasso temporale e come questa ha influito sulla datazione dei dati e sulla cronologia. Tuttavia questo problema è stato piuttosto ridotto, per il semplice fatto che oggigiorno quando un sistema si collega ad internet, viene automaticamente sincronizzato col fuso orario del paese d'appartenenza (che qualora non fosse impostato di default sarà adottato il +0 UTC di Greenwich). Una volta presa nota di tutti questi fattori si inizierà a ricostruire la "*time-line*" degli eventi che hanno coinvolto il dispositivo interessato.

A questo punto inizia l'anello più delicato della catena di custodia e punto focale di tutta la procedura, ossia iniziare le operazioni che impediscano che i dati vengano successivamente modificati o subiscano alterazioni. È in questo istante che si innesta l'utilizzo di quei "*tools*" particolari come duplicatori forensi, telemonitor , programmi ad hoc e ecc. per l'analisi sicura dei dati. Tuttavia in parallelo devono essere compiute anche altre attività. Infatti nel caso in cui si renda necessario asportare i dati è vitale evitare che quest'ultimi subiscano anche la più minima modifica. Per fare ciò, oltre ad usare i "*tools*" prima citati, bisogna isolare il sistema in maniera tale da impedire ogni eventuale e possibile ingerenza esterna. Quindi per prima cosa il dispositivo sarà scollegato dalla linea se questo è connesso attraverso la rimozione del cavo lan oppure spegnendo il modem se è attivo il Wi-fi. Così i rischi di accessi esterni con dispositivi remoti vengono

ridotti quasi a zero e non possono essere effettuate infiltrazioni telematiche che potrebbero compromettere l'integrità dei dati.

Passo successivo è quello di comprendere l'entità dei dati che potrebbero essere rilevanti ai fini delle indagini. Spesso uno stesso dispositivo (come nel caso dei computer d'azienda o quelli domestici) può essere utilizzato da più persone, perciò si dimostra superfluo una completa asportazione dei dati presenti nel sistema se l'indagine è indirizzata verso un solo individuo o è finalizzata a cercare uno specifico file. Stabilire questo determina la priorità se è opportuno iniziare prima con l'analisi e poi procedere con l'acquisizione dei dati o viceversa, anche se la prassi più diffusa, e anche la più corretta, rimane iniziare con l'abduzione e poi solo successivamente proseguire con i vari esami in laboratorio, poiché spesso e volentieri le analisi condotte in loco possono essere affrettate e generiche e potrebbero portare a conclusioni errate. Inoltre agire sul campo comporta la irripetibilità degli atti mentre i controlli sulle copie possono essere effettuati diverse volte senza creare possibilità di equivoci o sbagli. Comunque qualsiasi sia la via intrapresa, una volta giunti al momento del acquisizione, si dovrà fare una cernita dei dati prescelti ed iniziare l'operazione dai dati più delicati per loro volatilità e finire con quelli più sicuri.

Non vi è un ordine preciso o definitivo su quale sia l'ordine dei file da acquisire, tuttavia secondo le "*best practice*" della documentazione RFC3227 viene illustrato un esempio piuttosto comune su che iter seguire[76]:

1) cominciare acquisendo le memorie "*cache*" e se possibile i cookies;

2) si procede poi con tutto ciò che è presente al momento del ritrovamento nella memoria RAM, tabelle di Routin e tabelle di processo;

3) passare in seguito a dati che potrebbe interessare temporaneamente i file di sistema;

4) successivamente si acquisiscono i dati presenti negli Hard disk sia che essi siano fissi o periferici;

[76] G. Amato, V. Destito, G. Dezzani, C. Santoriello, *Op. Cit*. , pag. 179.

5) si acquisiscono eventuali log;

6) infine si analizzano e copiano eventuali memorie di Back-up se presenti e si prende nota di che configurazione ha il sistema e che tipologia di linea internet viene utilizzata, per ricreare successivamente in laboratorio una copia virtuale del sistema hardware ritrovato sulla scena del delitto e del software o degli eventuali server che venivano utilizzati[77].

In conclusione viene presa anche nota dei forenser che hanno trattato i dati e di chi sarà destinato a custodirli (se eventualmente il custode dovesse cambiare dovrà essere segnalato presso di chi e come è stato effettuato il trasferimento). Questa scala è stata elaborata con la ratio di voler dare precedenza a quei dati che più facilmente potrebbero essere persi per errori, imperizie (come ad esempio lo scollegamento forzato del cavo di alimentazione) o anche cause accidentali che esulano dall'essere (un calo di corrente o un black-out improvviso). Nell'eseguire la copia, o meglio la clonazione, dei dati viene effettuata l'ultima fase della "*Chain of Custody*". Infatti una volta adoperate le copie bit-stream dei diversi tipi di file per mezzo dei duplicatori forensi l'unica accortezza che si dovrà avere sarà quella di garantire un adeguato metodo di custodia e di utilizzo dei dati. La certezza sull'autenticità delle duplicazioni forensi e sulla loro conservazione viene ottenuta grazie alla "*funzione di hash*" e ai "*checksum*"[78].

Con il primo termine si intende una funzione matematica, utilizzato spesso anche nei sistemi di posta elettronica certificata, che in base al file che si ad oggetto elabora una stringa alfanumerica unica collegata ad esso. In questo modo viene ricreata una sorta di impronta digitale del file che lo contraddistinguerà da altri, poiché, qualora i dati subissero una qualsivoglia alterazione, ricalcolando la funzione di hash uscirebbe una stringa diversa dalla precedente. Gli algoritmi dei programmi che utilizzano questo tipo di funzione sono molto precisi e soprattutto quelli utilizzati dai forenser hanno zero margine d'errore poiché sfruttano un doppio algoritmo proprio per evitare collisioni, sicché se un file è certificato

[77] http://www.rfc-base.org/rfc-3227.html, "*Guidelines for evidence collection and archiving*", 2002.
[78] E. Forlani, *La conservazione preventiva di dati informatici per l'accertamento di reati*, in *Dir. dell'Internet*, 2008, Ipsoa.

attraverso questa tecnica la loro autenticità sarà piena ed avrà un'alta valenza probatoria.

Con il secondo termine si intende, tradotto letteralmente, una somma di controllo compiuta gradualmente mentre si compiono le operazioni d'analisi. In sostanza è una sequenza di bit sommata che, associata al pacchetto trasmesso, viene utilizzata per verificare l'integrità di un dato o di un messaggio. Verificando in un secondo momento il valore ottenuto memorizzato precedentemente con quello elaborato ripetendo l'operazione si avrà la sicurezza che non vi siano state modifiche se i due risultati coincidono. Tuttavia questa tecnica, al contrario della funzione di hash, non garantisce sempre l'integrità dei dati al 100%, ciò è dovuto al fatto che nel momento in cui si compie la somma vi possono essere bit con valore 0 oppure somme intermedie il cui risultato è 0, quindi possono essere introdotti facilmente altri bit camuffando il risultato finale. Inoltre anche se non fosse possibile aggiungere bit, il file potrebbe comunque essere cambiato modificando l'ordine dei bit, anche in questo la somma rimarrebbe uguale ma effettivamente sarebbe avvenuta una modifica (ad esempio invertendo le parole di un documento senza cancellarle o aggiungerle). È logico dedurre quindi che un qualsiasi reperto probatorio certificato solo tramite checksum non può essere considerato idoneo a formare la decisione del giudice in un processo, ma tuttalpiù potrebbe avere valore indiziario. Per fortuna col tempo questo sistema ha subito diverse influenze e studi per essere migliorato, e ad oggi si può dire che sono state create delle varianti che di certo si dimostrano più funzionali rispetto al metodo originale, come il "*checksum di Fletcher*". Questa tipologia di somma di controllo ha un algoritmo di calcolo più complesso e lento ma che da maggiori certezze per quanto riguarda l'integrità dei dati sottoposti ad elaborazione, questo perché nel computo della somma viene tenuto conto anche della posizione del bit, se vi sono eventuali bit dal valore 0 e se vi sono somme dal valore 0. In definitiva il mezzo adoperato è certamente tra i più affidabili in circolazione, ciò nonostante la prassi più comune, concorde con le diverse dottrine, è quella di prediligere l'uso della funzione di hash con doppio algoritmo, relegando l'utilizzo del checksum di Fletcher solo per il trattamento di alcuni dati per i quali l'impiego della tecnica di hash sarebbe superflua (ad esempio come pacchetti di dati che sono stati inviati via internet o download di software). Il documento RFC3227 infine conclude la

Chain of Custody con delle raccomandazioni generali da tenere presenti durante l'intera procedura, come porre particolare attenzione al momento in cui il dispositivo viene sconnesso dalla linea internet, perché potrebbero attivarsi programmi "*off the net*", oppure viene spento, assicurandosi di aver recuperato e acquisito tutti quei dati che potrebbero andare persi perché presenti solo nella RAM. In aggiunta viene ricordato di non di attivare programmi, sia che sia lo stesso sistema a consigliarne l'attivazione, sia autonomamente, per impedire che quest'ultimi causino modifiche o la cancellazione dei dati presenti nel dispositivo ad insaputa del forenser (naturalmente fanno eccezione i software non installati utilizzati da quest'ultimo essendo certificati e creati appositamente per mantenere inalterati i file).

2.3.2 *L'ammissibilità dell'informatic evidence*

Seguire con precisione e alla lettera le linee guida sicuramente nella maggior parte dei casi porta a risultati soddisfacenti e assicura che gli elementi probatori informatici ritrovati vengano valutati adeguatamente e considerati come se fossero originali ed affidabili. Tuttavia è bene specificare che non sempre l'esecuzione certosina di queste procedure porta ad un esito garantito. Questo perché alcuni dati, per la loro natura o per trattamenti antecedenti, potrebbero essere già danneggiati o comunque non rispondere conformemente a ciò che ci si aspetta dalle operazioni della catena. Oltretutto non è detto che ciò che è stato previsto dalle varie documentazioni di "*best practice*" sia sempre adatto ai casi che ci troviamo davanti, vuoi per le nuove tecnologie e tecniche criminose, vuoi per ragioni puramente fattuali dovute alle circostanze del caso. Ciò si ripercuote anche nel giudizio, poiché non si può addure alle prove in esame una validità assoluta solo per il fatto che le linee guida siano state rispettate. Le prassi internazionali, insieme a ciò che è previsto nel nostro codice di procedura penale, sicuramente sono una guida affidabile che garantisce un reperimento ed una tenuta funzionale della prova informatica per la sua particolarità, ma in gioco deve essere messo anche il raziocino e la bravura del forenser, che deve comprendere, "*cum grano salis*", quando, come e in che misura adoperare le indicazioni contenute nelle documentazioni per evitare di causare più danni rispetto a quelli che avrebbe

fatto se non avesse applicato le procedure, trasformando gli operatori in meri esecutori di istruzioni.[79] Non a caso vengono previsti, proprio per questo, corsi di aggiornamento e di studio per investigatori, forze dell'ordine e giuristi, per far sì che sviluppino competenze e senso critico nell'affrontare queste situazione. Inoltre l'odierna dottrina, attraverso manuali e mezzi di "soft law", diffondono sempre più quello che potrebbe essere definito una sorta di codice comportamentale, che un inquirente dovrebbe sempre tenere a mente ogni qual volta agisce sul campo ancor prima di mettere in pratica le best practice. Infatti non stupisce che la stessa documentazione RFC3227 evidenzia quali siano in realtà i criteri legali che devono essere soddisfatti affinché le prove sia riconosciute come valide, indipendentemente da quale procedura si sia eseguita[80]. Ragion per cui una "*informatic evidence*" potrà essere considerata *«ammissibile quando sia stata acquisita tramite strumenti che rispettino gli obblighi legislativi vigenti e supportata da idonea documentazione, mentre risulta autentica e completa se è possibile comprovare l'integrità attraverso, ad esempio, la verifica dei contenuti attraverso funzione di hash (checksum); l'autenticità e la completezza dovranno essere anche comprovate anche dalla documentazione della catena di conservazione. […] Potrà essere considerata attendibile solamente se non sussistono dubbi su come sia stata acquisita e successivamente manipolata, evitando che si possano sollevare dubbi in merito alla veridicità. La procedura di acquisizione potrà essere considerata completa e corretta: se descrive dove e come è stata rinvenuta la prova informatica; se è stato tenuto conto dell'ordine di volatilità dei dati nelle fasi d'acquisizione; se ogni fase è stata opportunatamente documentata, descrivendo anche le figure professionali intervenute nei loro compiti* »[81].

[79] L. Marafioti, *Digital evidence e processo penale*, in *Rivista Giuridica*, DeJure Giuffrè, 2011.
[80] M. Daniele, *La prova digitale nel processo penale,* in *Rivista di diritto processuale,* Anno LXVI (seconda serie) – n. 2, 2011.
[81] M. Tonellotto, Evidenza informatica computer forensics e best practices, in Rivista di Criminologia, Vittimologia e Sicurezza – Vol. VIII – n. 2, 2014; G. Amato, V. Destito, G. Dezzani, C. Santoriello , *Op. Cit*., pag. 183.

2.3.3 *La validità di elementi di prova video-fotografici digitali*

La tipologia delle prove fotografiche e videografiche è oggi diffusissima. Questo perché, aldilà delle riprese audio-visive che possono essere compiute da telecamere di monitoraggio e sorveglianza, tutti i dispositivi informatici, dai tablet ai cellulari finanche le consolle portatili di videogiochi, oramai sono dotati di fotocamere che permettono sia di scattare foto in ottima qualità sia di girare video della durata anche di diverse ore. La diffusione di immagini e video diventa esponenziale se poi si pensa che ogni persona condivide tutto questo materiale on-line attraverso i diversi social network (ad esempio "*Instgram*" è una piattaforma che si basa unicamente sulla condivisione di foto, mentre "*Vines*" di video). In questo panorama è scontato arrivare alla conclusione che, chiunque compie un atto criminoso, difficilmente riesce a sottrarsi alle fotocamere. Ma se da una parte vi è stata un'ampia diffusione di questo tipo di prove, dall'altra bisogna comprendere quale sia l'entità della loro utilità e soprattutto come devono essere valutate all'interno di un processo penale, considerando il fatto che, al pari di molte altre prove informatiche-digitali, possono essere modificate facilmente.

In passato le fotografie non prodotte digitalmente presentavano caratteristiche che le rendevano difficili da contestare e «*molto raramente veniva messa in dubbio l'autenticità di una immagine presentata come fonte di prova in un procedimento giudiziario. Nel caso in cui fosse stato necessario corredare un fascicolo di indagine delle relative fotografie, era comunque prassi depositare anche la pellicola da cui queste provenivano, i cosiddetti negativi. In realtà anche questi ultimi potevano essere alterati, sia agendo fisicamente sulla pellicola asportando od aggiungendo alcune parti e poi sviluppando l'immagine dal negativo modificato, oppure duplicando il negativo con una apposita strumentazione dopo avere applicato opportune maschere atte a nascondere od inserire i particolari voluti. In entrambi i metodi però, le modifiche erano rilevabili da un occhio esperto: nel primo caso era sufficiente esaminare il negativo modificato per notare i ritocchi, nel secondo si sfruttavano le diverse caratteristiche (grana, spessore) del negativo-copia, che per motivi tecnici non erano mai uguali a quelli*

dei rullini delle fotocamere»[82]. Con le fotocamere digitali le cose sono abbastanza diverse dato che l'immagine non prende subito fisicamente forma, ma esiste sotto forma di pixel in uno schermo. Ciò rende possibile sia vedere preventivamente l'immagine o il video catturato, e quindi successivamente eliminarlo se non soddisfacente, sia effettuare modifiche di filtro, taglio e montaggio senza neanche usare programmi specifici o professionali. In concreto quindi analizzare un file di questo tipo e capire se sia stato manipolato o meno può risultare molto ostico. Innanzi tutto nel momento in cui avviene il sequestro deve essere garantita la catena di custodia, in maniera tale da assicurare che qualora fosserò rilevate delle modifiche certamente quest'ultime risalirebbero a prima dell'intervento degli inquirenti. Successivamente devono essere controllate tutte quelle informazioni circostanziali al file (ossia i metadati), e confrontate con le informazioni che si possono trarre dall'immagine stessa (ad esempio risulterà insolita un immagine con un paesaggio invernale ma che risulta scattata in un periodo estivo, o immagini diurne che risultano scattate di notte, o ancora, qualora fossero indicate le coordinate geografiche, se ci fossero discrepanze con ciò che compare in foto). È possibile inoltre verificare la validità di una foto o di un video attraverso la presenza su di essi di particolari marchi rilasciati dai programmi di fotomontaggio o di certificazione. In alcuni casi questi elementi identificatevi sono piuttosto palesi poiché rilasciano delle sigle sul file modificato, in altri invece la traccia è pressoché invisibile ad occhio nudo ed occorre un esame forense informatico del file. In altri casi ancora, infine, apparentemente non si nota nessuna manomissione, ma il file può essere presente in un formato atipico oppure risulta un quantitativo di dati anomalo per quel tipo di file (ad esempio può essere stato compresso, procedura tipica dei programmi di fotoritocco, o una risoluzione grafica bassa). Tutto ciò fa dedurre che la foto o il video oggetto di analisi non sia quello originale o di partenza, ragion per cui ha subito dei ritocchi.

Appurato come sia possibile capire se e come una foto o un video sono stati alterati, bisogna successivamente comprendere in che termini ciò assume rilevanza in un processo penale. È normale e scontato che in casi di modifiche palesi e consistenti (come nel caso del 2010 delle "mozzarelle blu" che venivano

[82] S. Battiato, F. Galvan, *La validità probatoria di immagini e video*, in *Sicurezza e Giustizia*, 2013, pag. 30.

incriminati, attraverso foto ritoccate, anche i prodotti caseari di aziende in regola o che in realtà non presentavano questo problema) non è ammissibile che tali elementi di prova possano essere presi in considerazione. Tuttavia spesso possono essere considerate alterate anche prove che semplicemente hanno subito un doppio salvataggio, o ai quali è stato aggiunto un filtro per renderla più nitida. Sorge quindi l'esigenza di vedere come viene valutata dai giudici una prova audio-video che presenti delle manipolazioni. Secondo l'art. 189 c.p.p. «*quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona*», e riguardo le prove fotografiche "alterate" già più volte si è espressa la suprema corte di Cassazione[83] riconoscendo «*alle immagini fotografiche e filmate valenza di documento figurativo, del tipo testimoniale e diretto. […] La stessa giurisprudenza ammette, poi, in materia di prove filmiche l'utilizzo, anziché dell'originale, della copia del documento, quando emessa sia idonea ad assicurare l'accertamento dei fatti. Infine, il collegio replica alle obiezioni sull'utilizzo di fonti di prova, costituite da filmati che a dire della difesa non sarebbero ammissibili in quanto formati dalla giustapposizione di materiale vario, selezionato e montato […] sottolineando come questo non basti a determinare la loro non utilizzabilità, fatte salve la possibilità per le altre parti di addurre elementi idonei a dimostrare eventuali difetti di genuinità e manipolazioni arbitrarie delle immagini stesse*»[84]. In conclusione, quindi, la prova, se rispettati i requisiti imposti dalla legge e viene ammessa da entrambe le parti, può essere ritenuta valida dal giudice, anche se questa presenta delle alterazioni seppur minime. Per quanto possa sembrare un punto di vista atipico, tuttavia la scelta dei giudici è dettata dalle esigenze dei nostri tempi, che come dicevamo coinvolgono un gran numero di file fotografici e/o videografici e di altrettanti programmi di "*photoshopping".* Inoltre, il recente sviluppo di tecniche all'avanguardia nell'individuare eventuali falsi, fa si che non vi sia più preoccupazione nel rilevare prove che dovrebbero essere non ammissibili, per il

[83] Cass. Pen. Sez. V, Sent. n. 10309 del 18 ottobre 1993;
Cass. Pen. Sez. IV, Sent. n. 1344 del 13 dicembre 1995.
[84] Trib. Di Genova Sez. II, Ordin. n. 583 del 6 aprile 2004.

semplice fatto che possono essere ripulite facilmente dalle alterazioni e portate al loro stato originario[85].

2.3.4 *L'ammissibilità di un alibi basato su time-line e file digitali*

Essendo ormai i dispositivi informatici costanti del nostro stile di vita, quest'ultimi possono rivelarsi utili per ricostruire gli ultimi movimenti del rispettivo possessore e quindi creare le c.d. "*time-line*". Prendendo ad esempio sempre i cellulari di ultimi generazione, essi hanno al loro interno molteplici funzioni o software che possono garantire, o smentire a seconda dei casi, l'alibi di un indagato. Se il *device* è collegato alla linea internet, e/o a quella telefonica, è possibile sapere gli orari e il luogo in cui sono state effettuate delle telefonate o in cui è stato utilizzato un *browser* per effettuare ricerche sul web (inoltre i browser conservano in memoria anche la cronologia delle ricerche effettuate, ulteriori dati che potrebbero tornare utili in un'indagine). Se il dispositivo è anche dotato di GPS, e quest'ultimo fosse acceso, sarebbe anche possibile individuare la posizione geografica esatta del possessore. Infine ormai questo tipo di sistemi sono dotati di numerose e variegate applicazioni che ogni volta che vengono aperte, o utilizzate, registrano orario di accesso e a volte anche il luogo. L'esempio più diffuso è sicuramente quello delle applicazioni sui social network, come "*Facebook*", che nel momento in cui si effettua anche un semplice accesso o post costituito da parole, viene impresso orario e luogo geografico sul post stesso. O ancora vi sono molteplici applicazioni sportive o di fitness (come "*Runtastic"*) che, qualora attivate, dovendo misurare il movimento e le calorie giornaliere bruciate dal possessore, registrano posizione, tragitti compiuti, andatura, tempo ed altro. Queste sono tutte informazioni che, non solo in un'indagine possono rivelarsi molto utili per la loro precisione e il loro contenuto, ma presentano anche un alto grado di affidabilità essendoci zero rischi di alterazione, per il fatto che i programmi utilizzati per raccogliere i dati sono piuttosto sofisticati e difficili da craccare. Tuttavia, ad eccezione delle chiamate dove vi può essere una

[85] S. Battiato, G. Messina, R. Rizzo, "*Image Forensics. Contraffazione Digitale e Identificazione della Camera di Acquisizione: Status e Prospettive*", Chapter in IISFA Memberbook , 2009;
S. Battiato, F. Galvan, *Op. Cit*.

controprova vocale, tutte queste informazioni possono avere un vizio di fondo, ossia che ad avere compiuto le azioni registrate dal dispositivo posso essere stato qualcun altro diverso dall'indagato. Infatti lo smartphone può benissimo essere ceduto ad un terzo, che è a conoscenza delle credenziali di accesso alle varie funzioni, ed attivare appositamente diverse applicazioni. In questi casi, quindi, per avere la certezza che dietro determinate azioni vi sia sempre una determinata persona, bisognerà prima di tutto controllare quali soggetti sono i possesso delle credenziali di accesso del sistema (come detto precedentemente nel paragrafo sugli accessi on-line illeciti), in seguito si verificherà la plausibilità dietro determinati atti registrati dal cellulare (ad esempio risulterebbe improbabile che una persona in una condizione fisica precaria abbia compiuto degli spostamenti ad una certa velocità).

Altra tipologia di informazioni utilizzata per cercare di ricostruire una *time-line* è quella dei metadati. Si è già detto in precedenza che i metadati sono tutte quelle informazioni circostanziali legate ad un determinato file digitale. Solitamente ai fini di una ricostruzione di un alibi si utilizzano gli eventuali orari di apertura, modifica e chiusura del file. Nel caso poi di file o software che implicano la scrittura, la digitazione o anche il disegno e l'editing, è possibile calcolare effettivamente quanto tempo e con che costanza il soggetto ha lavorato con quel programma o sul quel file in base alla frequenza della pressione dei tasti o del progredire delle modifiche del file (naturalmente rapportate alla coerenza del file finale prodotto). Alterare i metadati può essere difficile, ma non così complesso da richiedere particolari competenze. Difatti esistono numerosi programmi che permettono di ottenere senza troppi problemi questo risultato. In tal caso bisogna verificare ogni volta, per quanto possibile, in primo luogo se vi sono anomalie rilevabili dal formato del file attraverso appositi software di analisi (come nella Digital-image forensics per le foto), ed in secondo luogo controllare la coerenza del file con i suoi dati circostanziali. Questo metodo pure assicura validità probatoria del proprio alibi con una certa sicurezza, ma sempre con la premessa che a quel determinato terminale posso avere accesso solo una determinata persona, o che a poter compiere quelle operazioni possa essere stato solo quel

determinato soggetto. Nelle diverse sentenze del caso Garlasco[86], grazie a questi controlli effettuati su un documento word incrociati con altre rilevazioni fatte attraverso le cronologie dei motori di ricerca, fu possibile ricostruire ed accertare con sicurezza che l'imputato, in determinato lasso di tempo, non poteva essersi mosso dalla sua postazione di lavoro da casa[87].

Infine vi può essere il caso un cui a sostegno di un alibi vengano usate delle immagini o delle riproduzioni video. Riguardo la loro ammissibilità e validità all'interno del processo si è già parlato nel paragrafo precedente. Tuttavia in queste sede è bene specificare che nonostante un file di questa tipologia venga giudicato idoneo ad essere acquisito, perché non presenta contraffazioni, devono comunque essere effettuati altri controlli particolari affinché questo materiale possa essere usato a sostegno di una time-line. Fondamentalmente bisogna verificare che, anche se non sono stati utilizzati programmi di editing, non ci troviamo di fronte ai c.d. "*falsi originali*". Quest'ultimi sono «*immagini che sono portatrici di un messaggio falso, pur essendo costituite dall'esatta sequenza di bit prodotta dall'apparato al momento dell'acquisizione. La problematica dei falsi originali merita una trattazione separata rispetto alla Image Forensics "moderna", sia per le differenti procedure realizzative, sia per i diversi approcci necessari al loro smascheramento che spesso sono più simili a quelli dell'investigatore dell'era "pre-digitale". […]si (può) parla(re) di falsi originali quando il file che contiene l'immagine od il video, pur veicolando un messaggio errato è costituito dall'originale sequenza di bit prodotti dal dispositivo di acquisizione. In questo caso, la falsa informazione che caratterizza il documento visivo è stata inserita prima dello scatto o della ripresa che stiamo esaminando*»[88]. Il risultato descritto dalla definizione può essere raggiunto, quindi, attraverso operazioni precedenti alla digitalizzazione. L'autore del falso può realizzare una scena artificiosa prima di scattare la foto o girare il video, in maniera tale da rappresentare qualcosa che apparentemente corrisponda al vero,

[86] GUP di Vigevano , Sent. del 17 dicembre 2009;
Corte di Assise d' app. di Milano, Sez. I, Sent. n.55 del 17 dicembre 2014;
Cass. Pen. Sez. I, Sent. n. 44324 del 31 ottobre 2013.

[87] V. Calabrò, G. Costabile, S. Fratepietro, M. Ianulardo, G. Nicosia, "*L'alibi informatico. Aspetti tecnici e giuridici*", Chapter in *IISFA Memberbook*, 2010.

[88] S. Battiato, F. Galvan*, Verifica dell'attendibilità di un alibi costituito da immagini o video*, in *Sicurezza e Giustizia*, 2013, pag. 47.

oppure effettuare delle sovrapposizioni o alterazioni ed in seguito digitalizzare il tutto. Nel primo caso è molto difficile scoprire l'inganno dietro quella che, al netto degli esami di Image forensics, è una prova genuina. In tal caso la ricerca degli investigatori deve basarsi nel ritrovare elementi contradditori o sospetti all'interno della "scena", come posizioni anomale o innaturali, vestiario non comune per i soggetti coinvolti, paesaggi insoliti e altri indizi. Nel secondo caso, invece, individuare le alterazioni pregresse può essere più semplice. Anche qualora i software di analisi non individuino modifiche apportate alla foto o al video, è possibile accorgersi dei fotoritocchi con un attento esame visivo e dei confronti. Infatti in questa tipologia di file è possibile rilevare solitamente giochi di luce fisicamente impossibile, punti di fuga differenti, inconsistenze geometriche ed altre incongruenze. Nei file video, poi, può essere ancora più evidente una manomissione, controllando eventuali asincronie o picchi di frequenza nella traccia audio, differenza di montaggio nelle pellicole (per esempio da digitale ad analogico), più inoltre tutti quei dettagli grafici già visti nell'esame di semplici prove fotografiche[89].

[89] Beyer, Stefanie, et al. "*Towards Fully Automated Digital Alibis with Social Interaction*", In *Tenth Annual IFIP WG 11.9 International Conference on Digital Forensics*, 2014;
S. Battiato, F. Galvan, *Op.Cit.*

CAPITOLO 3

Case study sulla ricerca delle prove

3.1 *Il Caso Garlasco e il suo iter travagliato*

Un contributo significativo nell'assimilazione della computer forensics è stato dato dai giudici che, attraverso la giurisprudenza, negli anni hanno saputo interpretare le disposizioni conformemente alla ratio con la quale erano state prodotte e colmato le lacune del legislatore; facendo si, inoltre, che ben aderissero al nostro sistema legislativo. In merito a ciò tuttavia è bene esaminare con particolare attenzione una delle vicende giudiziarie, ampiamente conosciuta per la risonanza mediatica per le gravi lacune investigative-informatiche che furono segnalate nel corso del processo, che più di ogni altra ha dimostrato quanto non solo siano importanti la computer forensics e le prove informatiche, ma anche come quest'ultime non posso essere ricercate con i "*modus operandi*" delle altre fonti di prova.

Ripercorriamo l'iter giudiziario: Alberto Stasi fu assolto per mancanza di prove nel 2009 dal Gup del Tribunale di Vigevano (la sentenza all'interno della quale venivano rilevate le mancanze investigative sul lato informatico). In seguito verrà nuovamente giudicato innocente "*per non aver commesso il fatto*" anche nel 2011 dalla Corte d'Assise d'appello di Milano. Nel 2013 la questione approderà presso la nostra Corte di merito che annullerà le precedenti decisioni con rinvio alla Corte d'appello, adducendo tra le motivazioni diversi elementi di prova rilevanti che non erano stati valutati nei precedenti gradi. Tuttavia la stessa Cassazione esprimerà le sue perplessità sulle indagini condotte, sottolineando la difficoltà di *«pervenire a un risultato, di assoluzione o di condanna, contrassegnato da coerenza, credibilità e ragionevolezza»*. Il 17 dicembre 2014, nel processo di rinvio presso la Corte d'appello di Milano, Alberto Stasi verrà condannato a

ventiquattro anni di reclusione, essendo giudicato colpevole, ma grazie al rito abbreviato la sua pena sarà ridotta a sedici anni, verdetto che infine, il 12 dicembre 2015, sarà confermato definitivamente dai giudici della Suprema Corte.

Il caso Garlasco, sia per la sua dinamica sia, come si è visto, per la durata delle indagini, ha coinvolto al suo interno molteplici elementi e fonti prova eterogenei. Per quanto riguarda le prove informatiche furono acquisite e valutate fin da subito, ma furono rilevate delle irregolarità. Il giudice del tribunale di Vigevano stabiliva che «*in data 14 agosto 2007 Stasi Alberto consegnava spontaneamente alla polizia giudiziaria il proprio computer portatile (marca "Compaq"). Da quel momento fino al 29 agosto 2007, quando il reperto informatico veniva consegnato ai consulenti tecnici del pubblico ministero che procedevano all'effettuazione delle copie forensi dello stesso, i «pervenire a un risultato, di assoluzione o di condanna, contrassegnato da coerenza, credibilità e ragionevolezza» carabinieri accedevano ripetutamente e scorrettamente (senza l'utilizzo, cioè delle necessarie tecniche forensi di indagine) alla quasi totalità del contenuto del computer. Peraltro, già nel verbale di polizia giudiziaria datato 29 agosto 2007 i militari indicavano alcune delle operazioni condotte sul personal computer di Stasi. In realtà le metodologicamente scorrette attività espletate su tale fonte di prova sono risultate, all'esito dei successivi accertamenti tecnici, ancora più consistenti: sette (e non cinque come riferito) accessi al personal computer di Alberto Stasi; non corretta indicazione dell'avvenuta installazione ed utilizzo di diverse periferiche USB (oltre a quella correttamente indicata); non corretta indicazione dell'avvenuto accesso al disco esterno in uso ad Alberto Stasi; non corretta indicazione di accessi multipli al file della tesi di laurea in vari percorsi di memorizzazione dello stesso: si vedano sul punto i rilievi del collegio peritale tecnico/informatico (ing. Porta e dott. Occhetti). Il complesso di queste alterazioni veniva rilevato anche dai consulenti tecnici del pubblico ministero (i Ris di Parma) nella loro successiva analisi. Pur tenendo conto di quanto sopra, i Ris, nella loro relazione tecnica e successive integrazioni e chiarimenti, concludevano sostanzialmente nel senso che il giorno 13 agosto 2007 il computer portatile di Alberto Stasi veniva acceso alle ore 9.36; quindi venivano aperte delle fotografie digitali fino alle ore 9.57 e dopo le ore 10.17 non sarebbero presenti tracce informatiche che comportino la presenza attiva di un utente che*

interagisce con il PC. Il consulente tecnico della difesa, nel merito, evidenziava che in realtà il file della tesi era stato aperto alle ore 10.17 e che quella mattina erano state ivi scritte e memorizzate due pagine della tesi di laurea. In presenza tuttavia delle alterazioni al contenuto informativo della fonte di prova a causa degli accessi scorretti dei carabinieri e della ritenuta conseguente impossibilità di provare con certezza quanto sopra rilevato, la difesa dell'imputato eccepiva l'inutilizzabilità come fonte di prova del contenuto del computer portatile in parola »[90]. Questa prima parte della sentenza evidenzia come la prassi investigativa italiana non sia stata delle migliori (argomento non nuovo nella giurisprudenza italiana evidenziato anche nelle sentenze del delitto Cesaroni[91]). Infatti ben difficilmente la Corte poteva ritenere valide le fonti di prova reperite sul campo poiché non solo non era stata adottata nessuna catena di custodia, ma addirittura, non usando neanche una strumentazione adeguata, si è giunti ad un'alterazione tale dei dati da non permetterne più una buona acquisizione successivamente. Esaminando bene gli errori, strettamente per quel che attiene l'ambito informatico dal punto di vista di un forenser preparato, iniziamo dal più grave, ossia gli accessi non sicuri. Indubbiamente qualsiasi raccolta di elementi di prova non può essere ritenuta valida se gli investigatori si approcciano al sistema informatico senza l'utilizzo di un *block witer,* un duplicatore forense o dei software, che permettono di introdurvi all'interno dei file senza operare modifiche anche solo cronologiche. Così facendo hanno compromesso l'intero alibi dell'imputato, non potendosi più stabilire quali accessi erano stati effettuati dal ragazzo e quali dagli organi inquirenti. Proseguendo, Stasi consegna di sua volontà il PC. Elemento non da poco vista la volontarietà del gesto e l'apparente rapporto collaborativo. Sicuramente si sarebbe potuto sfruttare meglio questo vantaggio chiedendo all'imputato maggiori credenziali, informazioni di acceso, particolarità e ecc. riguardo il suo computer. Infine le indagini si focalizzano quasi unicamente sulla cronologia della tesi in maniera tale da ricostruire i movimenti del presunto omicida. A parere di chi scrive l'errore è solo quello di concentrarsi unicamente sui meta-dati, ossia informazioni intrinseche ai file che possono avere riferimento al mondo fisico (il luogo, l'entità, il formato di creazione/modifica o

[90] GUP di Vigevano , Sent. del 17 dicembre 2009.
[91] Cass. Pen. Sez. I, Sent. n. 264 del 26 febbraio 2014.

appunto come nel nostro caso l'orario), e sottovalutando un'ulteriore prova informatica, ossia i cellulari sia della vittima che dell'indagato. Infatti un'adeguata e approfondita analisi dei dispositivi mobili non sarebbe stata di certo completamente inutile, giacché se ne era effettuata solo una limitata unicamente ai tabulati delle chiamate effettuate. Per ciò che riguarda le critiche mosse sul fatto che per il soggetto agente era possibile alterare piuttosto facilmente l'orario d'acceso ai suoi file, sia cambiando le impostazioni di fuso orario del suo PC (che se non opportunamente controllate per tempo può non rimanere traccia alcuna della modifica, soprattutto se essa è stata effettuata off-line), sia più semplicemente abducendo il sistema informatico dalla sua postazione e portandolo con se (operazione piuttosto semplice e di facile esecuzioni trattandosi di un PC portatile e quindi facilmente trasportabile ed utilizzabile all'esterno anche per lunghi periodi se provvisti di cavo d'alimentazione), furono da subito considerate come teorie alquanto improbabili. In merito a queste possibilità la Corte di Cassazione affermerà che veniva «*esclusa l'ipotesi che l'attività informatica rilevata il 13 agosto 2007 fosse svolta da Stasi fuori casa, valorizzandosi la limitata autonomia del computer per le modeste prestazioni della batteria, la difettosità del cavo d'alimentazione e la telefonata ricevuta dallo stesso da parte della madre alle ore 9:55 sulla utenza fissa di casa e durata 21 secondi, ed erano anche indicate le condivise ragioni esposte dal collegio peritale, che escludevano la volontaria alterazione dei riferimenti temporali del sistema, connesse alla necessità di conoscenze informatiche superiori a quelle accertate in capo a Stasi e alla sincronizzazione temporale delle medesime attività in rapporto anche alle telefonate effettuate e ricevute dal medesimo quella mattinata*»[92]. Argomentazioni dunque validissime che, anche a voler essere decisamente pignoli, difficilmente si potrebbero controbattere. Sebbene il PC di Stasi potesse raggiungere al massimo una durata di due ore di autonomia, sarebbe stato impossibile mantenere il dispositivo acceso per così tanto tempo, e in un altro luogo al di fuori della propria abitazione, mantenendo allo stesso tempo l'attività di scrittura del documento word della tesi costante (come è stato anche confermato in seguito dai tecnici attraverso le tempistiche di battitura dei caratteri e la mole di materiale all'interno del file). Per ciò che riguarda la possibilità

[92] Cass. Pen. Sez. I, Sent. n. 44324 del 31 ottobre 2013.

dell'alterazione dell'orologio interno, ammesso che il soggetto possedesse le adeguate competenze informatiche, sarebbe stato troppo arzigogolato far coincidere e sincronizzare l'apertura e la chiusura dei file visto che, seppur minimi, sono presenti anche degli intervalli. Inoltre si considera anche infattibile l'ipotesi di utilizzo di programmi da remoto, non disponendo l'imputato né dei mezzi, né delle capacità per adoperare questa via.

Tornando alla sentenza del Gup di Vigevano, in seguito il giudice si sofferma non a caso sulla natura particolare degli elementi probatori in questione e sulle loro particolari caratteristiche che necessitano appunto di un approccio non convenzionale , dicendo infatti che «*il documento informatico è connotato da un'intrinseca caratteristica di fragilità: nel senso che le tracce elettroniche sono facilmente alterabili, danneggiabili e cancellabili. Per questa ragione, può essere arduo (e ciò anche a prescindere da ipotetiche manipolazioni dolose ma perfino da eventuali comportamenti colposi posti in essere da chi interviene su di esso) conservare un documento informatico inalterato, in modo da assicurare che la prova sia autentica e genuina. Di qui la necessità di adottare particolari cautele, quali l'adozione di copie di hard disk conformi all'originale, che vengono rese non modificabili mediante appositi procedimenti tecnici. Al fine di ampliare la possibile valenza dimostrativa della prova informatica (c.d. digital evidence) superando alcune incertezze interpretative connesse ad istituti processuali disciplinati dal legislatore prima del consolidarsi sotto il profilo socio/culturale e scientifico dell'era informatica e nel contempo positivizzare questa imprescindibile esigenza (già ben conosciuta nella prassi) legata alla genuina acquisizione del documento informativo e alla successiva attendibile valutazione della prova informatica, la recente legge 18 marzo 2008 n. 48 (in esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica) ha, fra l'altro, modificato la disciplina di alcuni mezzi di ricerca della prova nel senso di estendere espressamente l'oggetto di questi anche ai sistemi informatici e telematici e ha prescritto, nel contempo, la necessità che il soggetto operante adotti idonee cautele tecniche che assicurino la conservazione del documento informatico e ne impediscano l'alterazione* »[93]. Senza aggiungere altro, in

[93] GUP di Vigevano , Sent. del 17 dicembre 2009.

quest'ultimo punto il giudice chiarisce l'importanza e allo stesso tempo la volatilità delle prove informatiche, ragion per cui, rimandando anche ai riferimenti normativi di recente novellazione che hanno introdotto la computer forensics, afferma più che mai la necessità dell'utilizzo di queste pratiche non solo ai fini di una corretta ed esaustiva indagine, ma per garantire quello che deve essere un equo e corretto processo conforme alle norme di legge.

Nonostante l'approccio inesperto, grossolano e per niente cauto da parte della polizia giudiziaria nel recuperare gli elementi di prova informatici, all'interno del processo poi si è cercato di porre rimedio alle irregolarità, per quanto possibile, attraverso perizie ed accertamenti tecnici ex post. Sempre il giudice di Vigevano infatti affermava che «*Non emergendo ragioni (e nemmeno la difesa dell'imputato, peraltro, prospettava tale evenienza) per affermare che in tali accessi ed operazioni sommarie da parte della polizia giudiziaria vi fosse stato un dolo di inquinamento probatorio di qualsiasi genere, siamo ragionevolmente di fronte ad errori di metodo compiuti, salva prova contraria, in totale buona fede. Ciò comporta due conseguenze di fondo. La prima: la questione se i risultati conseguiti correttamente (secondo il profilo metodologico) dai consulenti del pubblico ministero e della parte civile siano comunque ragionevolmente attendibili (ed in che misura) e/o se alcuni dati ed informazioni siano stati, invece, irrimediabilmente persi a causa, appunto, di tale iniziale errore metodologico da parte della polizia giudiziaria ha una valenza oggettiva. Nel senso che vi è il pericolo (e qui l'eccezione processuale della difesa dell'imputato assume una valenza di merito degna della massima attenzione) che Alberto Stasi non riesca più a provare il proprio alibi che invece, se fossero state salvaguardate al massimo l'integrità e genuinità del documento informatico, sarebbe riuscito per ipotesi a conseguire. Ma vi è ugualmente il pericolo, all'opposto, che il contestato (dalla difesa dell'imputato) grado di attendibilità del risultato (emerso dalla consulenza tecnico/informatica dei Ris di Parma) sulla falsità dell'alibi offerto dall'imputato (come indizio a carico dello stesso che andrebbe valutato alla luce dell'art. 192 c.p.p.) possa essere (in tutto o in parte) inficiato, appunto, dagli accessi ed operazioni sommarie di cui sopra.*

Dunque, una valenza oggettiva, appunto, in quanto emerge, in ultima istanza, il pericolo di un pregiudizio al fondamentale valore neutro dell'accertamento della

verità. Sulla base di queste considerazioni, una volta che l'imputato chiedeva di essere giudicato con le forme del rito abbreviato, affidare ad autorevoli professionisti del settore un accertamento peritale in materia diventava assolutamente necessario ai fini della decisione». La conclusione a cui il Gup giunge è piuttosto plausibile, se non del tutto scontata. Sebbene sia tacito da entrambe le parti che gli errori commessi dalle forze dell'ordine siano stati fatti in buona fede e senza l'intenzione di inquinare le prove, irrimediabilmente comunque quei dati hanno perso di affidabilità, non essendo possibile effettuare una cesura tra gli accessi di Stasi e quelli della polizia, e di conseguenza non essendo possibile utilizzarli né per confermare né per smentire l'alibi dell'imputato. *«il collegio peritale (ing. Porta e dott. Occhetti) evidenziava che le condotte scorrette di accesso da parte dei carabinieri hanno determinato la sottrazione di contenuto informativo con riferimento al personal computer di Alberto Stasi pari al 73,8% dei files visibili (oltre 56.000) con riscontrati accessi su oltre 39.000 files, interventi di accesso su oltre 1500 files e creazione di oltre 500 files. Insomma interventi che hanno prodotto effetti devastanti in rapporto all'integrità complessiva dei supporti informatici (in questi termini si esprime il collegio peritale). Queste alterazioni indotte da una situazione di radicale confusione nella gestione e conservazione di una così rilevante quanto fragile fonte di prova da parte degli inquirenti nella prima fase delle indagini ha comportato, in primo luogo, il più che grave rischio che ulteriori stati di alterazione rimuovessero definitivamente le risultanze conservate ancora nella memoria complessiva del computer. In secondo luogo, gli accessi in questione hanno comunque prodotto degli effetti metastatici rispetto all'esigenza di corretta e complessiva ricostruzione degli eventi temporali e delle attività concernenti l'utilizzo del personal computer portatile nelle giornate del 12 e 13 agosto 2007. Rispetto dunque ad altre questioni probatoriamente rilevanti (come, ad esempio, il movente/occasione dell'omicidio su cui torneremo nel prosieguo) non è più possibile esprimere delle valutazioni certe né in un senso né nell'altro: in questo ambito, il danno irreparabile prodotto dagli inquirenti attiene proprio all'accertamento della verità processuale»*[94]. La perizia effettuata dagli esperti apre purtroppo ad uno scenario impietoso e scoraggiante. Circa tre quarti della

[94] GUP di Vigevano , Sent. del 17 dicembre 2009.

totalità dei dati furono esaminati senza le dovute precauzioni. Ciò pur non portando ad un degradamento dei file o alla loro perdita, confermò tuttavia la loro inutilizzabilità *sic et stantibus* all'interno del processo.

Un punto di svolta nelle indagini si ha nel momento in cui i periti provano a ricostruire la cronologia dei movimenti di Stasi attraverso l'utilizzo di altri metadati combinandoli con gli orari degli altri eventi avvenuti e di cui si aveva una determinata valenza probatoria. Infatti «*il collegio peritale (ing. Porta e dott. Occhetti) riusciva comunque a ricostruire le attività compiute da Stasi Alberto quella mattina sul proprio computer portatile. Ciò sulla base dei seguenti passaggi. I periti avevano a disposizione in primo luogo la versione della tesi di laurea del 12 agosto 2007 alle ore 19.00 quando si verificava un crash del sistema che consentiva di rinvenire i files temporanei che attestano il lavoro pomeridiano alla tesi di laurea. Quindi una versione del 12 agosto alle ore 19.19 acquisita durante le operazioni peritali mediante la produzione di una chiavetta da parte dei consulenti tecnici dell'imputato. Questa versione della tesi riprodotta su tale supporto non presenta, come argomentato dal collegio peritale in udienza, delle anomalie e quindi può essere considerata come una versione della tesi che si colloca attendibilmente fra quella del crash e quella del 14 agosto 2007. Del resto, è ragionevole la condotta di Stasi che, avvenuto il crash, decide di cautelarsi salvando il proprio lavoro su una chiavetta esterna temendo un eventuale successivo disguido (anomalia bloccante che poteva generare ulteriori crash) del sistema operativo. Infine, la versione della tesi al momento del 14 agosto 2007 quando Stasi Alberto, avendo consegnato agli inquirenti il proprio computer, si presentava presso la caserma chiedendo loro di poter copiare la propria tesi di laurea su una pen drive. Dunque, schematicamente possiamo ricostruire il lavoro alla tesi nelle seguenti fasi: alle ore 19.00 avviene il crash di sistema (sul sistema si cristallizzavano tutti i files temporanei attivi in quel momento non essendo avvenuta una chiusura normale dell'applicativo word), quindi vi è il salvataggio della tesi sulla chiavetta esterna. Da quel momento il sistema rimane praticamente inattivo fino alle ore 21.28 circa quando viene riaperto il file della tesi fino alle ore 21.59; alle ore 22.14 viene ripreso il lavoro alla tesi fino alle 00.10 quando viene chiuso il file di Word e messo in standby il computer. La circostanza che l'attività sulla tesi di laurea sia stata eseguita*

anche successivamente al crash era, del resto, stata dimostrata dalla consulenza della parte civile (ing. Reale) che aveva evidenziato per la sera del giorno 12 l'inserimento nel dizionario personalizzato dell'utente informatico di due parole nuove "inerentemente" e "Garbarino". Dunque, se Stasi aveva lavorato alla tesi anche la sera del giorno 12 era necessario aspettarsi che vi fossero dei files temporanei che attestassero il lavoro della tesi in quel lasso temporale: la circostanza che, invece, gli stessi mancassero era indice inequivocabile di come l'equazione sostenuta dai consulenti tecnici del pubblico ministero -mancanza di files temporanei uguale provata assenza di attività sul computer per la mattina del 13 agosto- fosse logicamente e tecnicamente scorretta. Partendo da questo dubbio di fondo e tenuto conto della grave anomalia rappresentata dalle alterazioni del contenuto informativo dovute agli accessi dei carabinieri che ben potevano avere determinato la cancellazione delle normali evidenze presenti all'interno del sistema operativo, il collegio peritale (con la collaborazione dei consulenti tecnici delle parti) ricercava delle particolari informazioni che si trovano fuori del sistema operativo»[95]. In seguito quindi i tecnici si sono occupati di visionare ogni possibile dato informatico che potesse essere stato, anche involontariamente, modificato dall'imputato ma che allo stesso tempo potesse rientrare in quel un quarto di dati che non erano stati intaccati erroneamente dagli inquirenti. Alla fine fu possibile ricostruire una "*time-line*" piuttosto definita e precisa, poiché Stasi aveva visionato diverso materiale pornografico prima di lavorare alla tesi di laurea. I metadati all'interno delle foto e dei video, insieme a quelli del documento word della tesi riguardanti i nuovi termini inseriti, l'andatura della battitura e il confronto con lo stesso lavoro eseguito la sera prima dell'omicidio, permisero quindi di tracciare in maniera dettagliata tutte le operazioni compiute su quel dispositivo. Il risultato fu stabilire che l'imputato aveva acceso il sistema intorno alle 9:35, per un oretta visionava il materiale pornografico di cui disponeva, e poi per le 10:20 apriva il file word ed iniziava a scrivere. L'attività di scrittura rimane costante per due ore fino alle 12:20, ora in cui non viene più digitato nulla. Tenendo conto di queste informazioni, ed avendo accertato che le altre teorie su eventuali spostamenti del terminale o attivazioni a

[95] GUP di Vigevano , Sent. del 17 dicembre 2009.

distanza non erano fattibili, bisogna concludere che Stasi Alberto in quel frangente di orario non poteva essersi mosso da casa.

3.2 *Conclusioni sul caso Garlasco e altre questioni in merito di carattere informatico*

Nonostante gli errori di indagine e l'assoluzione nei primi due gradi di giudizio per insufficienza di prove, alla fine Stasi sarà condannato. Inutile negare che la verità processuale ricostruita e accertata è stata formata per buona parte dagli altri elementi di prova ritrovati, come le tracce di DNA, e la *"blood pattern analysis"* una tecnica di ricostruzione della *scena criminis*, basata sulla biologia e la fisica, attraverso le macchie di sangue ritrovate sul luogo. È stato il punto di svolta di molti casi, primo fra tutti, il caso Franzoni[96], ricerca dei tabulati telefonici e ecc. Sicuramente il ruolo giocato dalle prove informatiche è stato significativo, visto che alla fin fine hanno ricostruito parte dell'alibi e dei movimenti del colpevole, ma di certo il loro peso all'interno dei processi sarebbe potuto essere più significativo, aldilà degli sbagli commessi in partenza. È pur vero che all'epoca dei fatti le conoscenze e mezzi della computer forensics non erano quelli odierne (basti pensare che essendo l'omicidio avvenuto il 13 agosto 2007 ancora non era stata neanche ratificata la Convenzione di Budapest), tuttavia non si può fare a meno di pensare che di certo determinati interventi ed azioni sarebbero stati incisivi e avrebbero permesso un iter giudiziario sicuramente meno travagliato.

In primis si sarebbe dovuta effettuare una copia dell'hard-disk del computer. Nonostante il PC sia stato consegnato volontariamente dall'indagato, si sarebbe potuto evitare un sequestro così invadente praticandone appunto uno "*non indiscriminato*" e diretto ad acquisire solo i file più recenti e rilevanti. Oltretutto non furono praticati neanche esperimenti riguardo l'autonomia della batteria (che qualora fossero avvenuti si sarebbe potuto comunque utilizzare in alternativa un modello identico a quello della *scena criminis*), sicché un'analisi così prolungata

[96] Cass. Pen. Sez. I, Sent. n. 31456 del 21 maggio 2008.

dell'intero sistema, dimenticandosi tra le altre cose di fare una copia di back-up dei dati certificata, si concretizza davvero in un eccesso di zelo e dispendio di tempo e risorse pressoché inutile. In definitiva sa sarebbe potuta anche effettuare una ricerca più approfondita sulla cronologia on-line del pc e prendere contatti con il provider che forniva il servizio internet.

In secondo piano, sebbene fu sequestrato il terminale mobile nella sua interezza, non furono presi in considerazione diversi file (in particolare delle foto con amici della vittima e del colpevole), anche non recenti, che sia per il loro contenuto (indumenti indossati dai soggetti o segni particolari), sia per i loro metadati, avrebbero potuto dare un apporto considerevole a chiarire una situazione *pre-criminis*, che successivamente non è stato possibile recuperare o confermare, poiché nonostante furono sequestrate durante le prime indagini, successivamente caddero nel dimenticatoio e probabilmente furono eliminate.

Infine, pur essendo state effettuate delle intercettazioni telefoniche (anche se pure queste eseguite con dei ritardi), i cellulari non furono esaminati alla stregua di dispositivi informatici. Vennero chiesti i tabulati soltanto delle telefonate, mentre quelli delle chat furono richiesti troppo avanti nelle indagini (due anni dopo) quando ormai il gestore telefonico le aveva eliminate, non essendo più obbligato a conservarle.

Merita un'ultima menzione il ruolo assunto dalle fotografie pornografiche. Oltre ad essere state vitali affinché fosse possibile ricostruire gli eventi della mattina del 13 agosto 2007, la loro rivelazione fece scattare nei confronti di Stasi un'ulteriore accusa per il possesso di materiale pedopornografico (ritenuto anche a volte dai p.m. ragione di litigio tra i fidanzati e successivo movente dell'omicidio). Successivamente, sebbene vi fu un'iniziale condanna, nel processo per Cassazione del 2014 l'uomo sarà scagionato da queste accuse per insussistenza del fatto. Infatti il materiale rinvenuto all'interno del computer poteva essere considerato legale, mentre le foto incriminate non erano in realtà mai state scaricate, ma vi erano solo tracce rimaste nella ricerca dei software di download. Le foto furono inoltre utilizzate dall'accusa inizialmente per delineare un profilo disagiato dell'imputato, come quello di una persona che ha problemi ha relazionarsi con altre persone, soprattutto di sesso femminile. In realtà poi saranno anche utilizzate

dalla stessa difesa in più occasioni all'interno delle motivazioni dei ricorsi, indicando al contrario che, rispetto alla norma, Stasi non aveva dipendenze dal porno né possedeva quantità esagerate di materiale per un ragazzo di allora venti tre anni.

Concludendo il caso Garlasco ha presentato diverse mancanze, anche al di fuori dell'ambito informatico, dettate in parte dalla mancanza di una prassi investigativa adeguata, in parte dai ritardi e tempi troppo dilatati delle indagini. L'intera vicenda rimane comunque un ottimo terreno di studio ed un esempio, purtroppo in negativo, di come questa tipologia di indagini necessariamente debbano essere compiute seguendo determinate linee guida e standard.

CAPITOLO 4

La computer forensics in futuro prossimo e negli altri Paesi più avanzati

4.1 *Le possibili innovazioni investigative (Hardware, programmi, App per smartphone)*

Dopo gli attacchi terroristici del 11 settembre 2001 l'attenzione della ricerca scientifica si è concentrata in particolar modo sul cyber spazio e sulle tecnologie informatiche. Questo perché i disastri che si erano verificati erano stati in parte causati da deficit e lacune nel campo informatico, ma soprattutto si era sottovalutato il potenziale che tale tecnologia potesse avere. Quindi si arrivò alla conclusione che sebbene il "*world wide web*" fosse una risorsa incredibile che permetteva livelli comunicativi e sociali non indifferenti, dall'altro era necessaria una regolamentazione e un controllo adeguato che facessero in modo di evitare la nascita e la proliferazione di organizzazioni telematiche criminali e terroristiche. Ad oggi la collaborazione con numerosi istituti scientifici ha permesso di far fronte a questa esigenza elaborando sistemi e tecnologie in grado di effettuare ricerche sempre più accurate e specifiche e coprendo quasi interamente il mondo virtuale. Ciò nonostante ancora oggi esistono ancora zone grigie, se non del tutto nere, del mondo informatico che ancora sfuggono al controllo dell'autorità (come appunto il deep-web), o comunque vi sono gruppi di hacker (Anonymous, Lizard squad e ecc.) che continuano a muoversi in totale libertà e dimestichezza anche in quelli che potremmo definire ambienti sicuri e sotto controllo. Tuttavia nella casistica odierna è difficile riscontrare veri e propri attacchi informatici nei confronti di cittadini comuni, se non appunto in quei casi in cui i gruppi di criminali informatici fanno sfoggio della loro abilità attaccando grossi sistemi informatici di aziende multinazionali che coinvolgono si i comuni cittadini, ma

indirettamente. In definitiva oggi i più grandi studi ed approfondimenti delle indagini informatiche, nonché lo sfruttamento delle tecnologie più avanzate, sono compiuti in realtà dai grandi settori strategici dagli analisti (che attraverso la tecnica del "*data-meaning*" raccolgono informazioni in rete in diversi campi ai fini di protezione e pianificazione di eventuali attacchi esterni), più che dalle piccole procure[97]. Ciò non toglie che comunque di riflesso anche quest'ultime, con tempi piuttosto lenti, si stiano dotando dei mezzi adeguati. Tempi che potrebbero essere notevolmente ridotti se, per l'appunto, si affiancassero ai laboratori di scienza forense quelli di computer forensics. In questo modo si permetterebbe ai forenser di approfondire i loro studi anche al di fuori delle scuole di formazione, ma ancor permetterebbe la possibilità di ricerche ed indagini più accurate grazie alla creazione di device, app e programmi open-source che permettano di "*customizzare*" gli strumenti inquisitori a seconda delle situazioni[98].

4.1.1 *L'utilizzo nelle indagini dello smartphone*

Si è già detto più volte quanto ormai gli smartphone, ossia i telefoni di ultima generazione, siano così diffusi nella società odierna. La principale ragione di ciò, oltre che per un evoluzione del costume sociale che si adegua ai tempi, è da ricercare nella praticità ed utilità sotto più fronti di questi dispositivi. Questi strumenti non sono e non possono essere considerati semplicemente telefoni tascabili, dato che, oltre che chiamare e navigare in internet, possono svolgere diverse funzioni grazie alle applicazioni presenti su di essi. Per applicazione (conosciuta anche con l'abbreviazione "*app*", o come software applicativo) si intende quella serie di programmi specifici che permettono ad un computer di svolgere determinate funzioni. Spesso molte app di base sono già preinstallate nei nostri cellulari, come la calcolatrice, il registratore, Word, Excel, lettore multimediale e ecc., ma la maggior parte di esse vengono scaricate successivamente dagli appositi "*store*" a seconda del sistema operativo dello

[97] F. Corona, *Network Analysis e Data Mining, Nuove frontiere per l'intelligence tecnologica*, in *Gnosis rivista di Intelligence Italiana*, 2003.
[98] J. R. Vacca, Computer Forensics: Computer Crime Scene Investigation. Second edition, Charles River media Inc., 2005.

smartphone. In base alle proprie preferenze, in pratica, l'utente sceglie come modificare il proprio dispositivo, o meglio sceglie quali "*up-grade*" scaricare, sapendo che gli torneranno utili nella sua routine. Si stima che oggi il numero di app presenti sul mercato superi il milione e mezzo, è molte di esse vengono progettate appositamente per essere utilizzate in ambito professionale, o per facilitare determinati mestieri (l'esempio classico è quello dei capotreno odierni che controllano i codici dei biglietti attraverso lettori "*QRcode*" con i loro dispositivi). Ciò detto, non sarebbe anomalo o privo di efficacia, cominciare a pensare di utilizzare lo smartphone nelle indagini da parte degli inquirenti, attraverso applicazioni che facilitino la ricerca della prova.

Di per sé il cellulare ha già di base ottimi strumenti per un investigatore, anche qualora non si trattasse di un forenser. Si possono scattare foto della *scena criminis*, fare riprese video oppure registrare vocalmente persone interrogate per l'assunzione di informazioni. Tuttavia tutte queste operazioni possono anche essere svolte facilmente con altri strumenti, sicché la praticità di compierle con uno *smartphone* si risolverebbe solo nella maneggevolezza di avere tutto su un unico dispositivo. Tuttavia, anche queste funzioni classiche, potrebbero essere potenziate semplicemente aggiungendo dei programmi di certificazione. Infatti ciascuno di questi *"tools"* potrebbe produrre potenziali elementi di prova per il dibattimento, che qualora avessero una certa garanzia e validità, grazie al rispetto fin da subito della catena di custodia, sicuramente farebbero risparmiare molto tempo e lavoro agli inquirenti sia in laboratorio, sia durante il processo per la loro acquisizione.

L'innovazione in questo campo potrebbe essere raggiunta, in verità, attraverso l'utilizzo di determinati programmi già esistenti nei vari store o la creazione di app apposite per gli inquirenti, che facilitino le indagini o offrano nuove possibilità di ricerca. Ad esempio negli stati uniti sono diffusissime tre applicazioni che di consueto vengono utilizzate sul campo e che di certo anche in Italia darebbero il loro contributo[99]:

[99] T. Dees, *3 great police iPhone apps*, in *PoliceOne.com*, 2011 .

La prima si chiama *"LexisNexis Accurint"* ed è un database utilizzato dalle forze dell'ordine. In tempo reale è possibile consultare diversi dati anagrafici e informazioni riguardo i criminali schedati come: luogo di residenza, lavoro, trascorsi giudiziari, ultime transazioni e ecc. Solitamente per poter ottenere questi dati è necessario accedere a dei terminali fissi nelle questure o nelle procure. Con questo sistema, invece, è possibile effettuare riscontri in tempo reale dal proprio cellulare ed è particolarmente efficace in caso di controlli incrociati o monitoraggi.

La seconda è "*Write & Say*", ed è un programma di traduzione istantanea. Questa applicazione è particolarmente vantaggiosa nelle operazioni che coinvolgono persone di nazionalità differente con cui potrebbe essere difficoltoso comunicare, o effettuare l'assunzione di informazioni di probabili futuri testimoni al momento. Ciò è possibile poiché l'app permette, registrando intere conversazioni, di riconoscere la lingua parlata dal soggetto e tradurla nella propria, ed anche viceversa, convertendo testi, documenti e ecc. in file audio o Word della lingua della persona con cui si conversa. Il software è in grado di riconoscere ben ventinove linguaggi diversi, riuscendo anche a captare eventuali inflessioni o dialetti, adattandoli. Inoltre, una volta effettuata la registrazione, è possibile salvare il file audio come Mp3 oppure convertirlo direttamente in un file Word. Un ottimo surrogato di questo "*tool*", può essere Google translate. Quest'ultimo è una funzione che può essere utilizzata anche online (quindi senza effettuare neanche un download) attraverso semplicemente uno dei browser di ricerca di Google sia su un sistema fisso che mobile. Anche in questo caso è presente il "*detect language*" qualora vi siano dubbi sulla lingua parlata, ed è possibile sia scrivere o incollare il testo, sia registrare vocalmente la voce, per poi effettuare la traduzione in pochi secondi. Tuttavia a differenza di "*Write & Say*" le lingue disponibili sono solo quindici, e nel caso di traduzioni troppo lunghe potrebbero riscontrarsi degli errori concettuali o grammaticali.

Infine, ultima app degna di nota è "*Magic Plan*". Questo software è nato per produrre planimetrie per interni in maniera abbastanza rapida. Fondamentalmente può essere usato per riprodurre e studiare scene del crimine in poco tempo,

potendo effettuare tecniche di ricostruzione 3D dell'ambiente istantaneamente[100]. Il programma sfrutta la fotocamera del dispositivo cellulare per catturare la struttura lineare della stanza sovrapponendo le varie immagini e creando un modello virtuale della stessa. È necessario, innanzitutto, scattare foto a ciascun angolo e alle pareti, posizionandosi al centro (similmente a quando si effettuano foto in modalità "*panoramica*" per i paesaggi), in seguito l'applicazione elaborerà i dati visivi raccolti, tenendo conto anche di porte, finestre, e ecc. Il risultato che ne esce è abbastanza accurato e riporta anche determinate misure dell'ambiente che possono contribuire ad avere una visione più chiara dell'indagine. Anche in questo caso un grande vantaggio di questa applicazione, al pari delle precedenti, è la possibilità di esportare i dati raccolti in diverse tipologie di file, come PDF, JPEG e DXF(tipico formato per i progetti grafici e di disegno), che possono essere certificati e poi analizzati in un secondo momento o acquisiti all'interno del processo.

4.1.2 *Le principali applicazioni investigative di nuova generazione*

Le possibilità elencate finora di certo possono dare contributi significativi in un'indagine, ed accelerare i tempi delle analisi e le rilevazioni dei forenser. Tuttavia il vero potenziale dell'utilizzo di un sistema informatico portatile sta nello sfruttare risorse e funzioni che portino a risultati che non sarebbero raggiungibili attraverso i mezzi ordinari o convenzionali. Ciò è possibile grazie a dei software operativi *sui generis*, che, sebbene alcuni siano solo prototipi sperimentali, sono stati creati appositamente per forze dell'ordine e giornalisti, per investigare sul campo nel caso fossero presenti prove o indizi informatici[101]:

La più interessante di tutte tra le applicazioni investigative di nuova generazione è certamente "*Cree.py*" (un gioco di parole sulla parola inglese raccapricciante). Questo programma, in maniera molto embrionale, butta le basi per quelle che

[100] S. Battiato, F. Galvan, *Ricostruzione di informazioni 3d a partire da immagini bidimensionali*, in *sicurezza e giustizia*, 2013.

[101] P. Myers, *Data at Risk: How To Protect Your Sources and Your Work* , in *Global Investigative Journalism Network*, 2015;

P. Myers, *Online Research Tools and Investigative Techniques*, in *Global Investigative Journalism Network*, 2015.

potrebbero essere in futuro delle mini operazioni di sorveglianza di massa controllata. Il principale scopo dell'app è quello di ricercare una persona, o rilevare i suoi ultimi spostamenti, attraverso un'analisi incrociata dei diversi contatti sui social network che la persona indagata dispone. Basta immettere i principali dati identificativi ed una volta individuati gli account attivi, come ad esempio Facebook, Twitter, Instagram e ecc., il programma analizzerà foto, post, e geolocalizzazioni ed in breve può dare sia l'ultima posizione del soggetto con relativo orario, sia, qualora vi fossero abbastanza dati, mappare i percorsi abituali compiuti dal soggetto in esame. Naturalmente, affinché l'applicazione possa operare al massimo della sua efficacia, sarà necessario che la persona scomparsa o della quale si effettua la ricerca, abbia aperta sui social l'opzione che permette la condivisione delle informazioni geografiche (un'impostazione solitamente di default già attiva, ma che si può disattivare su richiesta). Unico problema che potrebbe sorgere, in merito all'utilizzo di questo sistema in Italia, è se sia o meno compatibile con la normativa sulla Privacy e il trattamento dei dati personali[102], dato che il software potrebbe fare un massiccio uso di file dal contenuto sensibile. In verità il problema viene risolto a monte, poiché spesso tutte le fonti a cui il sistema attinge per effettuare la ricerca sono social network. Ciò implica che l'utente di questi format, nel momento in cui si iscrive al suddetto , firma già un contratto con la clausola che specifica che ogni contenuto che verrà pubblicato sul social, diventerà pubblico e visibile sull'internet (naturalmente poi è possibile per ogni utente restringere a preferenza il campo di visibilità dei propri contenuti postati qualora lo desiderasse). In conclusione essendovi già una concessione a priori dell'utente, non si rischia di invadere la sua privacy visto che si utilizza materiale che lui stesso ha deciso di condividere, o per il quale non ha revocato il consenso per la pubblicazione[103]. Sicché il rischio di ricadere in un caso come quello del "*Datagate*", compiuto dalla NSA nel 2013, che utilizzava materiale sensibile tratto dai cellulari per l'osservazione dei cittadini, americani e non, senza autorizzazione, è pressoché inesistente[104].

[102] D.Lgs. del 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*".
[103] Trib. di Firenze Sez. II, Sent. n. 5675 del 8 gennaio 2015.
[104] G. Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, in *The Guardian*, 2013;
http://www.geocreepy.com/

Altri due programmi, particolarmente utili in indagini che riguardano siti web, sono "*IntelliTamper*" e "*Foca*". Entrambi hanno lo scopo di esaminare siti on-line per la ricerca di file, collegamenti ipertestuali e ecc., e creare una mappatura analitica dell'intero sito. Per quanto riguarda il primo software ha un interfaccia piuttosto semplice da usare. Una volta avviato ricerca tutti i materiali presenti sul sito, anche quelli nascosti, ed in seguito li espone nel layout base di Explorer. Affianco ad ogni elemento della ricerca, oltre al nome del file, comparirà anche la sua dimensione, formato e data dell'ultima modifica. I tempi di analisi dipendono dalla complessità del sito e purtroppo se ne può esaminare solo uno per volta se non si vuole rischiare di bloccare il programma[105]. Il secondo invece presenta delle complessità maggiori nell'utilizzo, ma di conseguenza da risultati più ampi e dettagliati, soprattutto da un punto di vista tecnico-informatico. L'applicazione è, infatti, in grado di rilevare maggiori informazioni nascoste rispetto alla sua controparte vista precedentemente, come domini correlati, proprietà del sito web, informazioni tecniche relative ai server, ed anche i metadati nei documenti presenti sul sito. Tutti questi file e dati possono essere scaricati, memorizzati e successivamente analizzati. Il programma è in grado di rilevare qualsiasi tipologia di documento, dai file PDF fino agli SVG, attraverso una ricerca che sfrutta tre motori di ricerca (Google, Bing, Exalead). Vista l'ingente mole di documenti che può essere raccolta, è possibile catalogare i file, ed aggiungere ulteriori informazioni di base per semplificare o aprire file particolari. La principale utilità del secondo programma rispetto al primo, oltre alla sua precisione, è la possibilità di comprendere l'origine di determinati file sospetti, e le ingerenze esterne da parte di altri server e client, che apparentemente non hanno a che fare o non sono direttamente collegati al sito principale[106].

Ultimo software degno di nota è stato creato da uno sviluppatore indipendente ed è chiamato "*GeoSetter*". La principale utilità di quest'ultimo sta nella capacità di tracciare su una mappa interattiva (simile a Google Earth) la posizione geografica delle foto sottoposte ad analisi. Il programma elabora tutti i metadati, principalmente data e ora, all'interno del file ed anche eventuali geolocalizzazioni. Nel caso di più foto di uno stesso ambiente è in grado di dare informazioni

[105] http://www.softpedia.com/get/Internet/Other-Internet-Related/IntelliTamper.shtml
[106] https://www.elevenpaths.com/labstools/foca/index.html#

davvero particolari ed interessanti, come la posizione del fotografo nel momento in cui la foto è stata scattata oppure la fotocamera, le impostazioni e il programma di fotoritocco utilizzati. Il programma può essere anche collegato a Google Maps, in tal caso sarà possibile ottenere informazioni riguardo il luogo dello scatto, come coordinate geografiche, foto correlate, dati ITPC ed altre eventuali tracce, e si può effettuare anche la sincronizzazione con altri siti di localizzazione e con le immagini simili ritrovate, ma in formati differenti[107].

Alcune di queste applicazioni, in verità, vengono già utilizzate in Italia, ma prettamente nell'ambito privato. Evidentemente, essendo le indagini condotte dagli investigatori privati di natura particolare, o comunque in parte con obiettivi diversi, e disponendo di mezzi di certo limitati rispetto a quelli delle forze dell'ordine, ciò ha fatto si che questi strumenti trovassero più diffusione e ampio consenso in questo bacino d'utenza, vista comunque la loro praticità e i costi relativamente bassi. A dimostrazione di ciò il fatto che oggi esistono delle vere e proprie "*community*" di investigatori-forenser che scambiano pareri, aggiornamenti e "*tools*" tra di loro, come la recente applicazione "*Investigazioni*" che, nata dalla richiesta di un'utenza di detective privati ed impostato sul modello del programma statunitense già sopracitato "*LexisNexis Accurint*", permette di rilevare, inserendo i rispettivi dati: se un auto è stata rubata dalla targa; se un documento è stato smarrito dall'ID; ogni informazione pubblica legata ad una persona. Tuttavia queste constatazioni sul panorama investigativo privato odierno, fanno comprendere quanto divario ci sia rispetto al modo di operare degli inquirenti del lato pubblico e di quanto ormai sia necessario per loro adeguarsi all'andamento dei tempi ed evolvere verso un nuovo tipo di indagine.

In ultimo è bene dire che nella fase delle indagini preliminari, come alternativa al mezzo delle intercettazioni, possono essere configurate alcune app che ben si prestano come surrogati a determinate situazioni di ricerca del mezzo della prova. Si parla principalmente delle applicazioni "*SpymasterPRO*" e "*Mcouple*". Entrambe, se installate su un dispositivo, permettono di controllare e visionare le conversazioni What's app e Viber di un cellulare, e nel caso del secondo software

[107] http://www.geosetter.de/en

è anche possibile esaminare contatti, mail, cronologia delle chiamate, posizione GPS e messaggi Facebook, il tutto in tempo reale. Il vantaggio principale di simili strumenti è sicuramente la facoltà di poter avere sotto controllo anche determinati canali di comunicazione tra i più usati (come appunto "What's App") che usufruiscono della crittografia "*end-to-end*", e quindi molto difficili da decodificare normalmente con mezzi convenzionali, o nel caso di gestori del servizio non collaborativi. Unico inconveniente è quello che, per attivare il programma sul dispositivo che si intende controllare, è necessario scaricare l'applicazione sul suddetto dispositivo, operazione alquanto difficile da compiere se l'obiettivo è anche quello di tenere all'oscuro di tutto ciò il proprietario. Qualora, infatti, il soggetto fosse consapevole di certo non utilizzerebbe più quelle funzioni o potrebbe fornirsi di un altro cellulare. Tuttavia in merito entrambi le app sono state progettate sia per essere camuffate e rimanere indiscrete durante l'utilizzo, sia per non lasciare tracce una volta cancellate[108]. Vista la grossa similitudine con i mezzi di intercettazione di comunicazioni e conversazioni, e soprattutto per i diritti che potrebbero essere lesi dal loro impiego, come quello della libertà e della segretezza delle comunicazioni o quello della privacy, le modalità di utilizzo delle applicazioni di questo tipo dovrebbero essere assoggettate interamente, con gli adeguamenti del caso, alla disciplina degli artt. 266-271 del codice di procedura penale, essendo equiparabili fondamentalmente alle intercettazioni del flusso di comunicazioni relativo ai sistemi informatici e telematici[109]. In questo caso sarebbero fornite le giuste garanzie non solo per la loro esecuzione durante il periodo delle indagini preliminari, ma anche in seguito durante le altre fasi del processo, per l'acquisizione e la validità delle prove eventualmente raccolte.

4.1.3 *Le principali applicazioni in ambito legale*

L'utilizzo dello smartphone e delle app dovrebbe essere uno standard ormai anche per chi pratica la professione forense. In un contesto dove ormai anche le modalità classiche del processo si stanno informatizzando e tutti i

[108] http://spymasterproreview.com/
[109] G. Conso, V. Grevi, M. Bargis, *Op. Cit*.

tribunali, anche i più piccoli, si stanno dotando di servizi telematici sui rispettivi siti online, sembra scontato che anche i giuristi si dotino dei giusti mezzi che gli permettano di tenersi al passo con i tempi. C'è da precisare che naturalmente le "*Legal app*", rispetto alle corrispettive usate dagli inquirenti o dagli investigatori privati, presentano caratteri più utili allo svolgimento della funzione professionale tra le aule di tribunale e nel proprio studio.

Innanzi tutto, anche in questo caso, ritroviamo applicazioni generiche che ben si prestano a facilitare i compiti di un avvocato. Fondamentalmente si tratta di normali software d'ufficio, come "*Dropbox*", "*ReaddleDocs*", "*Good Reader*", "*Penultimate*" e ecc., che permettono una vera e propria smaterializzazione dei documenti cartacei. Con i primi due programmi è possibile infatti condividere su delle cartelle online diversi materiali potendo accedere da diversi terminali, essendo necessari solo le credenziali d'accesso o un account condiviso. Nello specifico "*Dropbo*x" è una vera propria piattaforma Cloud, mentre "*ReaddleDocs*" è stata progettata appositamente per i documenti d'ufficio con la possibilità di poter memorizzare degli estratti. Per quanto riguarda le restanti, sono app utilizzate per la lettura di documenti PDF oppure per prendere annotazioni.

Venendo, invece, alle vere e proprie applicazioni legali, quest'ultime sono create con lo scopo principale di aiutare il libero professionista nel suo lavoro. Le opportunità sugli store online sono piuttosto variegate ed eterogenee. Principalmente questi programmi vengono prodotti dalle maggiori case editrici giuridiche, fornendo in primis una vastissima scelta di codici digitalizzati in ogni branca del diritto, in secundis strumenti per organizzare e preparare al meglio l'attività forense, come agende multitasking con non solo il profilo del cliente, ma anche i relativi dossier, calcolatori del contributo unificato, dei diversi tipi di tasso d' interesse e dei diritti di copia e ecc. Sono anche poi piuttosto diffuse diverse app dei principali tribunali italiani, prima fra tutte l'applicazione della Corte di Cassazione, che permette di consultare la giurisprudenza di legittimità ed avere in tempo reale aggiornamenti riguardo anche il Consiglio di Stato, la Corte dei conti, i Tar e ecc. Meno diffuse sono, invece, le applicazioni ministeriali. La più utile in

questo ambito è quella collegata al Ministero della Giustizia che permette di visionare i documenti negli archivi dei registri civili giudiziari. In merito sarebbero auspicabile innanzitutto un miglioramento di base dello strumento attualmente fornito dal Ministero, garantendo anche altri servizi diversificati, e successivamente uno sviluppo concreto di programmi utili legati anche alle altre istituzioni dello Stato.[110]

Volgendo, invece, uno sguardo al panorama statunitense, dal quale si può prendere ispirazione per delle innovazioni nel prossimo futuro, le risorse offerte si fanno più consistenti e numerose. Aldilà dei molteplici "*Legal Dictionary*" o programmi-archivio con la legislazione dei vari stati e la giurisprudenza della Corte Suprema, sicuramente le app più interessanti si dimostrano quelle improntate all'organizzazione della causa in tribunale e che quindi danno la possibilità di preparare il caso sia per la presentazione e la discussione in aula, sia al di fuori delle udienze. A seconda della tipologia possiamo catalogare le app in: applicazioni cosiddette di "*scanning*", che permettono di reperire velocemente copie dei documenti prodotti durante l'udienza attraverso la fotocamera; applicazioni di trascrizione, che permettono una facile registrazione di testimonianze, pareri di periti ed esperti e ecc.; le applicazioni "*Tracking*", che effettuano una scansione ed analisi del giudice di ogni distretto e dei giurati (alcune di queste applicazioni permettono perfino di monitorare le reazioni di quest'ultimi durante il processo, per permettere agli avvocati di perfezionare la propria arringa sui punti dove il sistema ha rilevato delle particolari reazioni); applicazioni database, che come già detto sopra servono principalmente ad avere sotto mano ogni tipo di documento o atto giuridico sotto forma di file; applicazioni di fatturazione, che calcolano il tempo e il numero di udienze dedicate ad ogni cliente, con il fine ultimo di stabilire l'ammontare dell'onerario; ed infine applicazioni specifiche a seconda del settore che si tratta, per esempio nel diritto di famiglia vi sono app che effettuano i calcoli per l'ammontare degli assegni di mantenimento.

Negli Stati Uniti poi sono piuttosto diffuse anche diverse app create direttamente da avvocati o professori per facilitare l'accesso del pubblico alla giustizia. Spesso

[110] G. Ziccardi, "L*'utilità delle app legali*", in *Diritto24*, 2013.

le classi meno abbienti non hanno la possibilità di affidarsi ad un professionista competente, ma, pur di non affidarsi ad un difensore d'ufficio o avviare cause che potrebbero rivelarsi onerose, preferiscono difendersi da soli attraverso i consigli e l'aiuto dei suddetti programmi. Questo fenomeno è dettato in buona parte da ragioni economiche, non solo quelle del cittadino indigente, ma anche e soprattutto quelle degli studi legali che utilizzano le app come biglietto da visita e successivo tramite di collegamento per attrarre a se tutti quei potenziali clienti latenti. Ma c'è da dire che questo sistema sta cominciando a portare diversi benefici, primo fra tutti un alleggerimento del carico di lavoro di diverse Corti anche le più piccole. Ciò accade grazie al maturare di una maggiore conoscenza giuridica di base riguardo le piccole questioni legali che potrebbero sorgere tutti i giorni, come un ricorso riguardo una multa o controversie condominiali. Le applicazioni che più riescono ad adempiere in questo scopo, come "*Ask a Lawyer: Leagal Help*" o "*BernieSez*", sono quelle che offrono un servizio di chat operativo ogni ora che permettono al soggetto interessato di chiedere una consulenza veloce, fornendo addirittura la possibilità di postare via Cloud documenti, immagini o file che possano rendere più chiara la causa, oppure ricevere pareri da diversi studi legali a seconda di chi si interessa al caso, il tutto gratuitamente. Vi sono poi applicazioni molto più specifiche che vengono create per aiutare determinati gruppi di persone, come una sorta di collettori per potenziali Class-Action o sindacati, come "*Disastr*" creata appositamente per aiutare chi rimanesse coinvolto in disastri o calamità naturali, o anche"*My Health Care Wishes*" nei casi di pazienti che hanno subito disservizi sanitari. Infine vi sono app che sono collegate direttamente con le forze dell'ordine o le altre istituzioni federali, e le funzioni che svolgono servono prettamente a creare una maggiore sicurezza o comunque a facilitare i compiti della polizia. Un chiaro esempio di ciò sono le applicazioni "*FBI Child ID*", "Sex Offender Search" e "*Stop & Frisk Watch*". La prima è un programma creata dal "*Federal Bureau of Investigation*" per creare una rete di comunicazione in tempo reale nel caso di sequestri di persona che prendono di mira bambini e ragazzini. Attraverso di essa è possibile contattare degli addetti i quali, dopo aver ricevuto informazioni, immagini e tratti salienti del soggetto scomparso attraverso un sistema di Q&A, operano immediatamente per emettere comunicati stampa al fine di informare ed attivare gli agenti nella ricerca e sensibilizzare la collettività. La seconda è un applicazione con un ruolo

precauzionale, anche se per certi versi potrebbe essere assimilata ad una sorta di *black list*. Scaricandola è possibile sapere generalità ed aspetto fisico dei molestatori già segnalati alle autorità. I dossier sui diversi malintenzionati possono essere aggiornati da ciascun utente registrato, aggiungendo anche informazioni più dettagliate come la frequenza delle infrazioni, i quartieri maggiormente colpiti, il numero di avvistamenti di un soggetto ed anche le accuse che pendono su di esso con relative testimonianze. Il sistema è inoltre direttamente collegato con il registro nazionale sui "*sex offender*" in maniera tale che possa sempre rimanere aggiornato in tempo reale. Sul modello di questa app vi sono poi anche ulteriori piattaforme, volte sempre alla prevenzione e all'informazione del cittadino riguardo eventuali ricercati evasi o non ancora catturati. Infine la terza applicazione è un software creato per evitare abusi da parte delle forze di polizia. Fondamentalmente permette di effettuare registrazioni in maniera piuttosto semplificata attraverso dei semplici movimenti del cellulare nel momento in cui si subisce un fermo o un arresto, potendo tornare utili in secondo momento durante un processo, se si rinvengono ad esempio delle incongruenze nei verbali o nelle dichiarazioni degli agenti. Tuttavia il programma funge anche sia da raccordo per raccogliere informazioni riguardo il numero di fermi ed arresti sospetti o avvenuti non secondo le procedure convenzionali nei diversi distretti, sia da *legal dictionary* tascabile sui diritti e le garanzie della persona sottoposta ad arresto.[111]

4.2 *L'utilizzo e la diffusione della computer forensics negli altri Stati*

Nel precedente paragrafo si è parlato molto del fatto che la maggior parte delle sperimentazioni e delle innovazioni provengano principalmente dagli Stati Uniti d'America. Nonostante vi siano realtà sociali molto più avanzate tecnologicamente, e quindi teoricamente con un potenziale maggiore, ad oggi la realtà giuridica americana è quella non solo più all'avanguardia nel campo di mezzi e metodi di computer e Digital forensics, ma anche quella che al meglio sfrutta le *digital evidence* nei propri processi. La ragione della diffusione capillare

[111] J. Dysart, *20 apps to help provide easier access to legal help*, in *American Bar Association Journal*, 2015.

di questo approccio investigativo e giuridico è da ricollegare più che altro alle cause storiche di come è nata quest'ultima. Difatti questa disciplina prese forma nei laboratori di informatica del FBI durante gli anni 80. Sebbene ancora il world wide web non esisteva, nelle case erano già particolarmente diffusi diversi elaboratori elettronici, che stavano diventando utensili ormai di uso domestico. Da questo nacque l'esigenza, sempre più grande, di specialisti che sapessero utilizzare tecniche dell'investigazione classica ma riadattate al mondo informatico. Essere arrivati per primi a queste conclusioni ha permesso all'ordinamento americano di assimilare al meglio il connubio tecnologia-giustizia. Ciò è comprovato dalla situazione di molti altri Paesi avanzati che ancora, da un punto di vista legislativo e giuridico, non sono aggiornati sotto questo aspetto (come ad esempio il Giappone, dove solo recentemente il governo ha iniziato ad approvare delle leggi quadro per regolare la responsabilità dei Provider, ed il rapporto di collaborazione tra essi e le forze dell'ordine). In sostanza affinché le tecniche di computer forensics possano aderire in maniera adeguata al tessuto normativo di una nazione non basta solo un adeguato progresso tecnologico, ma anche un ordinamento abbastanza recettivo alle novità legislative e che poi sappia metterle in pratica. All'uopo, quindi, può essere utile visionare l'esperienza di alcuni stati in merito, iniziando da quello americano che ha fatto da capostipite, fino alle comunità che solo recentemente si stanno aggiornando in questo ambito.

4.2.1 *L'esperienza negli U.S.A. e in Inghilterra e i loro casi più famosi*

Come brevemente accennato pocanzi, negli States l'esigenza di dotarsi di nuovi mezzi investigativi di ambito informatico-digitale nacque già quando verso la fine del 1970 ci furono diversi casi di frode finanziaria tra diversi stati federati. Durante le indagini le Corti degli stati coinvolti sottolinearono più volte che tutti i registri, e le relative prove collegati ad essi, erano unicamente presenti su computer. Da questi eventi si fece sempre più evidente la necessità sia di creare unità specializzate nel campo telematico, sia che i tribunali cominciassero a considerare le prove digitali al pari di quelle canoniche. Fu così che cominciarono a sorgere non solo i primi corsi di formazione per gli agenti federali, ma anche i

primi interventi legislativi volti a disciplinare il fenomeno, come il *Florida Computer Crimes Act del 1978*. Iniziarono anche ad essere creati i primi "*tools*" che avrebbero permesso di eseguire indagini adeguate e una catena di custodia per garantire l'acquisizione degli elementi di prova di fronte ai giudici, fino ad arrivare al 1984 quando la FBI fondò quello che oggi è conosciuto come "*Computer Analysis and Response Team*" o c.d. CART (che nel 2003 registrò più di 6500 casi, e l'esame di circa 782 terabyte di dati) [112]. L'anno successivo, quasi in contemporanea, in Inghilterra verrà creata in parallelo una sezione specializzata che sarà affiancata alla squadra anti frode della *Metropolitan Police* britannica. Infatti, anche in Gran Bretagna, prima della diffusione delle linee guida e degli standard internazionali, sempre per ragioni riguardanti crimini di frode la realtà giuridica si stava evolvendo per far fronte alla situazione. Al tempo le Corti e gli investigatori inglesi presero a modello di garanzia delle "*good practice*" stilate dal *Association of Chief Police Officers* (ACPO), che istruivano riguardo l'integrità e l'autenticità di una prova digitale.

Dagli quegli anni in poi, in entrambe le culture, la ricerca, l'esame e l'acquisizione delle *digital evidence* divenne uno standard necessario in qualsiasi situazione gli inquirenti si trovavano, andandosi quindi a specializzare anche in settori diversi da quello finanziario. Molti casi, anche famosi, trovarono una risoluzione solo grazie a questo metodo di indagine e all'ammissione delle relative prove. Alcuni dei più notori sono, ad esempio, "*l'omicidio Lopatka*", un apparente caso di omicidio del consenziente avvenuto nel North Carolina, dove si riuscì ad incastrare il colpevole, Robert Fredrick Glass, per omicidio volontario attraverso la copiosa corrispondenza via chat tra la vittima e l'assassino, che evidenziava la tendenza omicida e perversa di quest'ultimo, e del materiale pedopornografico presenti sul PC di lui (sul quale anche sarà condannato per il loro possesso). O ancora il "*Serial Killer BTK*" che fu, invece, uno dei primi casi dove furono decisive le analisi dei metadati, in quanto l'omicida, Dennis Rader, durante i sedici anni di attività (nel quale uccise dieci persone in Kansas) inviò alla polizia delle lettere in formato floppy-disk, grazie ai quali fu possibile risalire al nome dell'autore e al luogo di provenienza. Nel regno unito fu emblematico il

[112] I. Charters, *The Evolution of Digital Forensics: Civilizing the Cyber Frontier*, CC, January 2009.

recente caso di "*Krenar Lusha"*, un immigrato clandestino albanese che progettò di compiere degli attentati verso alcune banche inglesi. Nonostante l'arresto non era possibile accusarlo della premeditazione degli attacchi terroristici, poiché le uniche prove fisiche erano delle taniche di benzina, finché sul suo PC non furono ritrovati dei manuali digitali su come costruire bombe e altri dispositivi pericolosi e dei video riguardo esecuzioni, nonché delle testimonianze su alcuni siti di dating dove il criminale si vantava di essere un terrorista. Infine ultimo caso, che ha segnato una svolta per le indagini forensi, fu nel 2009 il processo alla Corcoran Group, conosciuto anche come la decisione "*Einstein and Boyd v 357 LLC and the Corcoran Group, et al."* della Corte Suprema di New York. In questa vicenda furono distrutti diversi documenti informatici volontariamente prima del contenzioso dai registri telematici dell'azienda, che potevano essere potenziali prove. Purtroppo i forenser non furono in grado di recuperare il suddetto materiale, tuttavia viste le modalità d'esecuzione, fu possibile almeno provare non solo che la cancellazione era avvenuta volontariamente, ma anche si era cercato di alterare i fatti. In questo modo fu creato un precedente nella giurisprudenza americana[113] riguardo l'adeguata conservazione e tenuta di eventuali elementi di prova informatiche da parte delle parti durante lo svolgimento del processo.[114] Sulla base di questi avvenimenti entrambe le nazioni hanno sviluppato un'accortezza non indifferente ed una maggiore specializzazione nelle questioni legali legate ai crimini informatici, o che coinvolgano sistemi telematici, rendendole oggi due dei maggiori "*influencer*" in questo campo in ambito di direttive internazionali.

4.2.2 *Le esperienze asiatiche, in particolare quella cinese, giapponese e coreana*

Il continente asiatico rappresenta un esempio piuttosto atipico riguardo l'evoluzione della computer forensics e delle sue *best practice*. Ciò è dovuto principalmente all'incredibile sviluppo economico e tecnologico che alcuni di

[113] Supreme Court of NY, Einstein v. 357 LLC, 604199/07.
[114] E. Casey, *Digital Evidence and Computer Crime*, Second Edition, Elsevier, 2004.

questi Paesi stanno avendo nell'ultimo ventennio, che li ha portati a dotarsi di apparati giuridici all'avanguardia in ogni settore. Difatti fino ai primi anni 2000 non solo non vi erano leggi in merito a reati informatici ed eventuali prove informatiche, ma in verità non si avvertiva proprio un'esigenza riguardo una legiferazione in merito, probabilmente dovuta al fatto che il problema della criminalità informatica era sentito in minor modo rispetto alle altre parti del mondo. Tuttavia dopo l'attentato del 11 settembre 2001, anche gli stati asiatici cominciarono a dotarsi dapprima di misure contro il cyber terrorismo ed eventuali cyberwar, in seguito di adeguate misure giuridiche che prevenissero e sanzionassero atti criminali collegati ai dispositivi informatici e telematici.

In Cina i primi interventi concreti furono effettuati nel 2004, quando nelle università legate alle forze dell'ordine iniziarono ad essere inseriti corsi di Digital forensics, e un anno dopo nel 2005 quando verrà fondato il *China Committee of Experts on Computer Forensics* (CECF), un'organizzazione nazionale volta in primis alla ricerca e allo sviluppo di nuove tecniche e nuovi mezzi da adottare nelle indagini e che siano ritenute valide e garantite nei processi. In secundis si occupa della diffusione di corsi di aggiornamento in materia di computer forensics in tutto il territorio cinese, dell'organizzazione di convegni e conferenze per sensibilizzare l'opinione pubblica riguardo la messa in sicurezza dei propri sistemi informatici ed infine di aprire uffici e centri informativi nelle città più grandi a sostegno del cittadino. La CECF collabora anche con altre organizzazioni, sia nazionali che internazionali, forze dell'ordine ed industrie tecnologiche per condividere tecniche e risorse, e garantire un adeguata sicurezza dagli attacchi informatici sia interni che esterni. Nel 2009 furono poi adottate misure ancora più severe e all'avanguardia. Ciò fu dovuto principalmente al rilascio nel 2006, ad opera di Li Jun un programmatore di Hubei insieme ad altre otto persone, di un virus *worm* piuttosto sofisticato. Quest'ultimo aveva un altissimo livello di diffusione grazie alla capacità di insinuarsi in ogni tipo di file, di sfruttare le risorse di rete condivise e di resistere alla maggior parte degli anti-virus in circolazione, e mise in seria difficoltà le autorità cinesi che cercarono di debellarlo dal web. Questo caso, che oggi viene ricordato come "*Panda Burning Incense*" (nome nato dall'icona che assumevano i file una volta infettati), fu la scintilla che convinse la Cina a prendere seri provvedimenti contro la criminalità informatica,

ma soprattutto ad effettuare un aggiornamento della propria legislazione in merito all'acquisizione delle *digital evidence* e alle catene di custodia. La principale innovazione fu la modifica al codice di procedura penale cinese, che avvenne il 14 marzo 2012, dove, con l'aggiunta di quarantacinque nuovi articoli, saranno introdotte le prime regole sulle prove informatiche, nonché i criteri per valutarle e ritenerle attendibili all'interno del processo e requisiti per giudicare determinate prassi investigative come garantite. In seguito l'intero sistema legale sarà adatto alla computer forensics entrando in linea con gli standard internazionali[115]. Nonostante poi il primato di Stati uniti e Regno Unito in questo campo, ad oggi la Cina conta i migliori laboratori di *Data-Meaning* e *Cloud-Computing*, ossia il settore dell'analisi e del calcolo dei dati depositati sulle piattaforme Cloud online.

Per quanto riguarda, invece, la situazione giapponese, essa per certi versi ha seguito un'evoluzione simile a quella cinese, ma con un incremento tecnologico superiore, dovuto principalmente ad una politica di sviluppo economico più aperta nei confronti degli altri Paesi rispetto all'altra potenza asiatica, che portò ad un iniziale scambio di risorse e conoscenze soprattutto dal versante americano. Tuttavia ad oggi, sebbene aggiornato e molto simile a quello italiano, l'approccio giuridico giapponese presenta caratteri piuttosto classici nei confronti dei crimini informatici. Il sistema giudiziario è diviso in sei Corti (Supreme Court, High Court, District Court, Family Court, e Summary Court), ogni prefettura ha il proprio tribunale (ad eccezione di Hokkaido che ne ha quattro), ma a seconda delle problematiche da affrontare il caso può essere assegnato a tribunali specifici con determinate competenze, come ad esempio accade per il diritto di famiglia o per le questioni inerenti la proprietà intellettuale. I reati informatici o collegati ad un sistema informatico vengono considerati al pari di reati convenzionali, sicché, a seconda della gravità e della prefettura in cui vengono compiuti, vengono assegnati ogni volta ad una Corte diversa. D'altra parte ogni Corte è dotata di personale altamente qualificato ed istruito per ciò che riguarda l'ambito informatico-telematico, sia che siano inquirenti o giudici. Prima del 2006 i reati informatici erano di competenza esclusiva forze dell'ordine ordinarie, ossia della *National Police Agency* (NPA), che, attraverso i suoi sette bureau distribuiti tra le

[115] K. P. Chow, F. Law, Y.H. Mai, *Understanding Computer Forensics Requirements in China Via The "Panda Burning Incense" Virus Case*, in *Journal of Digital Forensics*, Security and Law, 2014.

prefetture e la polizia metropolitana, ricopre tutto il territorio nipponico. Oggi la NPA è supportata nelle indagini dalla *High-Tech Crime Technology Division*, sottostante alla *Info-Communication Bureau,* che si occupa di visionare ogni caso di cybercrime. Dal punto di vista investigativo, quindi, il Giappone presenta un assetto piuttosto integrato, competente ed esperto, favorito probabilmente dalla partecipazione fin dai primi anni 2000 ad operazioni contro il crimine informatico nell' Interpol ed un progresso tecnologico non indifferente, che lo rendono il principale punto di riferimento asiatico in materia e il terzo stato al mondo, dopo U.S.A. e U.K., più avanzato in questo settore. Inizialmente la frode informatica, al pari degli altri stati occidentali, era il reato più diffuso nella nazione e comportavano circa un terzo del totale dei crimini che avvenivano in internet o sfruttando quest'ultimo. Tuttavia questo dato è andato lentamente scemando, lasciando oggi il primato ai reati di prostituzione minorile attraverso siti di dating e la diffusione di materiale pedopornografico (fino al 2009 vi era stato un incremento del 91% portando ad un totale di 944 casi annui per la prostituzione minorile e 647 per la diffusione di materiale osceno e pedopornografico). Ciò ha portato ad una maggiore attenzione e specializzazione delle autorità nipponiche verso la Digital forensics, il settore della Computer Forensics completamente incentrato sulle indagini digitali online, e la Computer Security, ossia le tecniche e le operazioni volte alla prevenzione del proprio sistema telematico e del cyberspazio. Naturalmente questa evoluzione ha toccato non solo la categoria delle forze dell'ordine, ma anche quella degli avvocati, che, in concomitanza con le recenti riforme legali varate dal governo volte a regolare la responsabilità dei provider, hanno dovuto aggiornarsi e specializzarsi nell'ambito di questa materia, essendo il processo giapponese principalmente incentrato sull'escussione delle prove e la loro eventuale concordanza o contraddizione. Attualmente il rapporto tra avvocati e specialisti forenser è di venti a uno, che rispetto a molti altri stati è un rapporto piuttosto considerevole considerandolo al pari delle statistiche americane, con la differenza tuttavia che il numero pro capite di avvocati giapponesi è più basso di quelli degli altri stati. Infine negli ultimi anni il Giappone sta adottando politiche di governo sempre più attente ai pericoli di una cyberwar esterna, e i recenti interventi legislativi ancora in corso, dovuta principalmente alla pressione dell'opinione pubblica, la ricerca tecnologica e

quella accademica, sono il segno di un'integrazione sempre più consistente nell'ordinamento.[116]

In conclusione, trattando anche della Corea del sud, sebbene anche qui i primi veri sviluppi arrivarono nei primi anni 2000, quest'ultima gode di un sistema giudiziario all'avanguardia ed ha probabilmente uno degli assetti organizzativi migliori al mondo a livello strategico-informatico per combattere il cybercrime. Fondamentalmente ogni crimine o indagine che coinvolga mezzi informativi rientra nelle competenze del "*Cyber Bureau of Korea National Police Agency*"[117], una sezione specializzata delle forze dell'ordine nata nel 2014 dopo diversi atti di sensibilizzazione fatti al governo coreano da parte dell' Interpol per far fronte ad eventuali problemi di cyber terrorismo. Lo scopo principale di questa istituzione è quello di mantenere sicuro per le persone e la loro privacy il cyber spazio, attraverso monitoraggi attenti del web e operazioni soprattutto di prevenzione per minimizzare i danni, favorendo lo sviluppo e la ricerca nel campo tecnologico-investigativo e collaborando con altre autorità sia nazionali che internazionali (molti, infatti, sono state le missioni, i "*symposium"* riguardo linee guida e prassi comuni e gli scambi di informazioni avvenuti in collaborazione con la FBI, ed anche altre organizzazioni più grandi come il G20). Il Cyber Bureau è diviso in tre divisioni, ognuna a sua volta suddivisa in altre sezioni a seconda delle competenze specifiche che sono necessarie. La prima è la *Cyber Safety Division*, che si occupa prettamente della sicurezza del web attraverso l'analisi delle minacce, la pianificazione di eventuali misure di sicurezza, fornire servizi di protezione e gestire le collaborazioni con le altre istituzioni. La seconda è la *Cyber Response Division*, il centro investigativo vero e proprio dell'organizzazione, sia per le indagini online che per i reati che coinvolgono sistemi informatici, inoltre vi sono tre sottosezioni specifiche per i reati finanziari, per i reati con finalità terroristiche e per l'organizzazione preventiva di strategie di investigazione. Infine la terza divisione è il *Digital Forensics Center*, il centro dei laboratori di ricerca dove vengono analizzate le prove informatiche a seconda della loro fonte, ossia mobile o pc, ed anche qui vi è una sottosezione

[116] J. Liu, T. Uehara, *Computer Forensics in Japan: A Preliminary Study*, in *Availability, Reliability and Security, ARES '09 International Conference on*, 2009.
[117] http://www.netan.go.kr/eng/index.do

organizzativa del lavoro da svolgere ed un'altra dedita allo sviluppo di nuovi "*tools*" per gli inquirenti. La presenza di un apparato così ben organizzato ed integrato nel loro ordinamento rende oggi la Corea una nazione con un altissimo livello di sicurezza informatica. Ciò è stato possibile tuttavia grazie alla grande sensibilità della popolazione coreana al potenziale pericolo del crimine informatico, più che per lo sviluppo tecnologico-giuridico (famoso fu il caso dei "Nuri-cops" del 2012, una squadra di ben 800 volontari che si occuparono di cercare e segnalare materiale pedopornografico per poi essere censurato dalle forze di polizia), che ha fatto sì che l'integrazione a livello legislativo avvenisse in maniera immediata e risolutiva.

4.2.3 *I primi approcci alla computer forensics nelle Nazioni di recente industrializzazione*

Diversi stati africani, medio orientali o del sud-est asiatico, piccoli e di recente nascita o che da pochi anni hanno ottenuto l'indipendenza, stanno vivendo negli ultimi anni un progresso e uno sviluppo economico considerevole. Queste nazioni, che nell'ambito delle analisi socio-economiche vengono considerate nella categoria "*newly industrialized country*" (NIC), vivono in contemporanea alla rapida espansione economica e dei mercati anche una crescita significativa dei loro diritti civili e della tecnologia.

Uno degli esempi più notori è il caso della Malesia, dove dal 2009 al 2010 si è registrato un aumento esponenziale degli utilizzatori di internet (da un terzo di tutta la popolazione si è passati ai due terzi), nonché conseguenzialmente una proliferazione raddoppiata dei principali reati informatici come la frode e commerci illegali. In risposta la nazione ha da subito aggiornato le proprie istituzioni, come i diversi ministeri maggiormente interessati, le forze di polizia e le agenzie legali, con personale che fosse competente ad affrontare le nuove minacce, istituendo anche il *Malaysia Computer Emergency Response Team* (MyCERT) un dipartimento che provvede a garantire servizi di sicurezza informatica ed assistenza da crimini informatici ai cittadini. Sebbene il governo malese stia finanziando ed incoraggiando la ricerca in questo campo, attualmente

il più grande problema dei forenser specialisti è quello di non poter usufruire dei *tools* adeguati nelle indagini. Non di rado accade, infatti, che molti crimini sia compiuti con tecnologie estere all'avanguardia, ma anche se compiuti con mezzi ordinari spesso gli inquirenti incontrano difficolta. Questa discrepanza è dovuta anche sostanzialmente alle tecniche utilizzate, che richiedono eccessivo tempo per produrre effetti concreti. Basti pensare che nel campo della Digital forensics, quando è necessaria un' analisi o una valutazione di materiale fotografico o video, si riscontrano problemi se queste si presentano in formati non ordinari o customizzati, essendo gli operatori abituati a trattare solo con formati tradizionali avendo poca esperienza in merito. Non a caso nel processo penale, i procedimenti riguardanti le prove informatiche sono affidate completamente agli esperti delle agenzie legali a cui fanno affidamento le parti. I tribunali effettuano solo un controllo di garanzia attraverso un professionista che assiste alle diverse operazioni e tiene aggiornato il fascicolo riguardo il caso e il suo stato di avanzamento, nonché fa si che le parti comunichino tra di loro ogni volta che viene effettuata una perizia. I punti di riferimento nel compiere vari rilevamenti durante le indagini sono unicamente gli standard internazionali dettati dalla documentazione RFC3227, mentre per gli esami e le analisi in laboratorio vengono seguite le linee guida *ASCLD/LAB International requirement*. A tal proposito il Paese sta varando nuove riforme legali che riguardino il ruolo degli specialisti di computer forensics, una disciplina più precisa ed adeguata per la *digital evidence*, la penalizzazione di determinati reati ancora non previsti ed infine maggiore attenzione alle possibile cooperazioni internazionali. In definitiva, nonostante il problema del *cybercrime* sia stato avvertito in Malesia già dalla metà degli anni 2000, e fino ad oggi le minacce sono state contenute con risultati abbastanza soddisfacenti, solo recentemente il governo ha deciso di dedicare fondi e risorse in questo settore, provvedendo alla futura progettazione di un centro di Digital forensics e cercando di approfondire la specializzazione nell'analisi dei cellulari, sistemi mobili, video e audio digitali, ma soprattutto il recupero dei dati da sistemi danneggiati.[118]

[118] A. Ariffin, J. Slay, H. Jazri, *Digital Forensics Institute in Malaysia: the way forward*, in *Digital Evidence and Electronic Signature Law Review* 9, 2012.

Altro Paese emergente che si sta approcciando al metodo della computer forensics è la Repubblica del Sudafrica. Questa nazione ha iniziato il suo periodo di sviluppo nel periodo post apartheid, in concomitanza con le prime elezioni democratiche e l'attuazione delle prime manovre di politica monetaria volte a ristabilire il debito accumulato dai precedenti governi. L'attuale situazione sudafricana non è ancora delle migliori, considerando che in molte zone ancora vige uno stato di povertà e arretratezza non indifferente. Ciò nonostante si è reso necessario prevedere nell'ordinamento norme ed istituzioni incentrate sui crimini informatici. Il più grande provvedimento legislativo in materia fu il *The Electronic Communications and Transactions Act* 25 del 2002. Questa riforma ha previsto l'introduzione di nuovi reati, come l'accesso non autorizzato ad un sistema telematico, della definizione di prova informatica, integrandola tra gli elementi di prova canonici all'interno di un processo, e della regolamentazione riguardo il mezzo di prova delle intercettazioni e il tenere sotto osservazione una persona. In merito alla penalizzazione degli accessi non autorizzati, la norma si è focalizzata principalmente su tre elementi del reato: l'accesso, i dati e la mancata autorizzazione. In tutti e tre i casi il legislatore sudafricano ha fatto si che per le definizioni non ci fossero riferimenti specifici, che potessero diventare obsoleti facilmente in un paio d'anni, ma nozioni incentrate sugli scopi di ogni singolo atto dell'azione. Per cui ad esempio non viene data una descrizione o un elenco dei tipi di accesso, ma viene definito tale ogni operazione volta ad ottenere, visionare, raggiungere e ecc. dei dati informatici. Per quanto riguarda, invece, l'inserimento della *digital evidence* nel processo penale, quest'ultimo era un passaggio evolutivo necessario per mettere al sistema di essere all'avanguardia rispetto ai tempi. Innanzitutto vengono definite le fasi basilari della catena di custodia, ponendo l'accento sulla garanzia che il materiale analizzato non venga compromesso né nella sua acquisizione né nel suo esame. Tuttavia alle prove digitali, per essere considerate ammissibili, non vengono applicate solo le disposizione della riforma, ma quest'ultime in combinato disposto con i requisiti legali imposti per le prove in generale. In seguito viene sottolineato il bisogno che determinate pratiche vengano eseguite esclusivamente da professionisti con le adeguate competenze e da nessun altro, e ciò vale soprattutto per le parti. Per poter richiedere ed esaminare questa tipologia di prove è, infatti, necessario avere un'apposita autorizzazione legale in maniera tale da rispettare e garantire

determinati diritti e le informazioni sensibili all'interno del dispositivo. Secondo le norme introdotte dalla riforma ciò è possibile nel momento in cui o si dispone del consenso del proprietario dello strumento o è stato emanato un mandato di perquisizione o, infine, nel caso in cui vi è stata una citazione in giudizio e viene richiesta dal giudice l'esame del dispositivo come probabile elemento di prova.[119] Nel territorio sudafricano sono poi presenti svariate società private nate in contemporanea con le prime riforme legislative (la più notoria di tutte è la *Cyanre (Pty) Ltd*[120]), che si occupano di fornire diversi servizi alle parti di un processo, inerenti soprattutto la Digital forensics, la garanzia della catena di custodia e la valutazione preventiva di una *digital evidence* all'interno di un contenzioso. La ragione della loro presenza dimostra come i normali studi legali non possano permettersi di avere nel loro personale dei forenser, necessario d'altra parte, secondo la loro legislazione, per avere accesso alle prove informatiche durante il contenzioso. In un bilanciamento di interessi, la domanda per i casi che coinvolgano sistemi informatici è talmente bassa da non ritenere opportuno un aggiornamento di questo tipo, sicché i piccoli professionisti non ritengono proficuo dotarsi personalmente di specialisti ma risulta più conveniente affidarsi alle suddette società decisamente più preparate e fornite, trattandosi comunque di attrezzature e tecniche che determinano costi iniziali non alla portata di tutti. In conclusione, quindi, la particolarità che rende interessante l'esperienza della Repubblica Sudafricana, distinguendola non solo dalle altre nazioni in via di sviluppo ma anche da quelle più evolute in questo settore, è l'attenzione smisurata sui soggetti che possono accedere ai dati digitali reperiti durante un'indagine, sia da un punto di vista di competenze pratiche che di garanzie legali per la tutela del contenuto nelle suddette.

Infine ultimo stato rientrante nelle NIC che merita menzione è sicuramente il Brasile, poiché sebbene è una delle poche nazioni emergenti ad avere dei riferimenti normativi solidi in materia, d'altra parte nella realtà dei fatti riscontra diverse difficoltà pratiche. Lo stato federale sudamericano ha un ordinamento legislativo che ricalca principalmente i modelli di civil law europei, e difatti, per

[119] J. Jordaan, *Ensuring the Legality of the Digital Forensics Process in South Africa*, in *International Journal of Computer Applications*, (0975 – 8887) Volume 68 n. 23, 2013.
[120] http://www.cyanre.co.za/about/history/

le regole nel campo della computer forensics, quest'ultimo non ha una legislazione propria ma si appoggia quasi completamente agli articoli della Convenzione sul Cybercrime del Consiglio d' Europa del 2001 [121]. In particolare, per ciò che riguarda il reperimento, la preservazione e la custodia della *digital evidence*, segue gli artt. 16,17,18 e 19 della Convenzione. Questo sistema crea non pochi inconvenienti, essendo spesso le definizioni delle disposizioni citate incomplete o comunque molto generali, essendo necessaria un'integrazione attraverso un intervento del legislatore. Ad esempio le norme in esame non fanno differenza tra dati di traffico, dati digitali memorizzati su un dispositivo, dati di log e ecc. creando incertezza sull'approccio tecnico che ogni volta si deve intraprendere quando si effettua un sequestro, non essendo contemplata tra l'altro la possibilità di un'acquisizione in tempo reale dei dati di traffico. Tuttavia, come nel caso dell'esperienza sudafricana, vi è anche qui una particolare attenzione a come è possibile accedere a queste informazioni, trattandosi perlopiù di autorizzazioni a visionare le postazioni informatico-telematiche sulla *scena criminis*. Per ottenere questi dati solitamente vi è bisogno di un ordinanza della Corte interessata, ma nel diritto brasiliano non vi sono leggi che permettono ad un'autorità competente di emettere un provvedimento che richiede ad una persona o ad un gestore di servizi di consegnare informazioni sui propri clienti e i loro dati. Inoltre, secondo le normative brasiliane sulla privacy vigenti, questo tipo di informazioni vengono considerate sensibili e da proteggere, e ciò fa si che per ottenerle sia necessaria sempre un'ordinanza del tribunale prima di poter essere comunicate agli inquirenti. Ragion per cui i sequestri di questo tipo di materiale probatorio sono ordinati insieme al mandato che autorizza l'acquisizione delle suddette prove, ma, come detto precedentemente, essendovi diverse lacune sul recuperare i file garantendo la genuinità e l'integrità degli stessi, spesso i risultati non sono dei più soddisfacenti. Altro problema della realtà brasiliana è il rapporto tra forze dell'ordine e i Provider. Quest'ultimi per legge non sono obbligati a conservare alcuna traccia dei registri di connessione. Inoltre, a causa della legislazione inadeguata, la maggior parte dei gestori ritengono che i log di connessione e le informazioni sui propri clienti siano protette dalla legge sulla privacy. La combinazione di questo stato di cose legale, unito alla mancanza di

[121]Convention on Cybercrime of the Council of Europe, European Treaty Series - No. 185, 2001.

tempestività da parte del sistema giudiziario brasiliano nell'effettuare determinate operazioni, spesso porta a situazioni in cui ormai non è più possibile ottenere quelle informazioni perché sono state già cancellate quando l' ordinanza del tribunale raggiunge i diretti interessati. Nel caso in cui, poi, i Provider siano situati all'estero, la situazione si complica ulteriormente, poiché per richiedere le informazioni è necessario effettuare una petizione attraverso una rogatoria internazionale, operazione dai tempi decisamente lunghi a meno che non esistano già degli accordi che semplifichino il recupero del materiale (come attualmente vi è tra Google e il Public Attorney's Office di San Paolo). Per ovviare a questi problemi sono state istituite in Brasile diverse organizzazioni, come il *Brazilian Internet Management Committee* (anche detto "*Comitê Gestor da Internet no Brasil*" composto dal governo e rappresentanti della comunità accademica e del settore privato) o l'associazione brasiliana dei Service Provider di Internet (c.d. ABRANET), con lo scopo di emettere raccomandazioni o autoregolamentazioni in maniera tale da sopperire alle lacune legislative. Tuttavia entrambi i provvedimenti non hanno forza di legge, di conseguenza le forze dell'ordine brasiliane non hanno mezzi per far rispettare o richiedere la conservazione dei dati degli indagati, dovendo far unicamente affidamento sulle singole politiche di ogni gestore, qualora sempre quest'ultimo sia collaborativo. Questa situazione, infine, si ripercuote anche sui mezzi di ricerca della prova come le intercettazioni telematiche. Esse sono equiparate alle intercettazioni telefoniche, ma in pratica, sia per i problemi con i Provider sia per ragioni di insufficienza di mezzi e competenze, vengono adoperate raramente. In conclusione, per ciò che riguarda il sistema giudiziario, quello brasiliano è fortemente ispirato al modello statunitense, essendovi sul territorio Corti federali e Corti statali con relative giurisdizioni e competenze (ad esempio i crimini legati alla diffusione di materiale pedopornografico sono affidati alle Corti federali). Ad oggi la polizia federale brasiliana ha circa centocinquanta esperti di computer forensics distribuiti tra tutti i ventisette stati brasiliani. Gli agenti di polizia dei vari stati ricevono la stessa formazione dei membri della *Brasilian Federal Police,* in maniera tale da non creare dislivelli di conoscenze e compromettere le indagini. Principalmente la maggior parte delle loro mansioni in questo settore è l'analisi delle prove digitali non direttamente legati alla criminalità informatica, come ad esempio i computer sequestrati durante le indagini su reati finanziari, frodi bancarie e la diffusione di

materiale pedopornografico. Tuttavia attualmente la polizia federale è al lavoro per creare un' unità specifica solo per i crimini informatici.[122]

[122] E.R. de Carvalho, *The Criminal Justice Response To Cybercrime*, in *140th International Training Course Participants'Papers*, 2008.

CONCLUSIONI

L'apporto dato dalle tecniche di computer forensics è stato sicuramente quello, in primo piano, di permettere al nostro ordinamento, come anche a quelli esteri che le hanno adottate, di essere aggiornato ed all'avanguardia rispetto alle nuove contingenze. Ai nostri giorni non è pensabile che un sistema giuridico moderno sia privo di una legislazione adeguata sui reati informatici, considerata la crescita graduale e tendente al suo aggiustamento nell'ultimo decennio. Come non è sostenibile che autorità competenti e professionisti del settore palesino carenze ad approcciarsi con protocolli pragmatici sia ai crimini canonici commessi mediante mezzi informatico-telematici ed ancor più alle nuove fattispecie emerse. Tutto ciò tenuto conto che i beni giuridici degni di tutela messi a rischio da questa tipologia di crimini sono di una certa rilevanza, ed hanno solitamente dinamiche che permettono di raggiungere una moltitudine di persone con estrema facilità ed in termini di tempo immediati. Dalle stime, infatti, risulta che gli italiani vittima dei cyber criminali, per un ammontare di 2,5 miliardi di danni all'anno, sono circa 9 milioni e per la maggior parte sono reati che aggrediscono il patrimonio, la libertà personale psico-fisica o morale sia di persone adulte che di minori, la libertà e la segretezza della corrispondenza e la protezione dei dati sensibili. Abbiamo ben visto, altresì, che il più importante contributo dato dalla computer forensics è quello di rendere le indagini degli inquirenti più celeri e precise sotto vari aspetti, poiché gli elementi di prova che si rinvengono con questi mezzi sono molto dettagliati, ricchi di informazioni eterogenee e, se acquisiti correttamente, impossibili da confutare dal punto di vista della validità. Tutti fattori che si ripercuotono in modo indubitabile a beneficio dei tempi processuali, ovviamente qualora non vi siano nelle fasi di escussione e valutazione delle prove dubbi o incertezze sulle modalità d'acquisizione del materiale che viene presentato. Per converso nel "case study" sull'omicidio Garlasco, emerge chiaramente che trascurare queste prassi sia stato oltremodo dannoso e deleterio per un contenzioso. Una mancanza di accortezza come quella esaminata mostra perché sia facile perdere diversi elementi di prova che fin da subito avrebbero dato svolte significative nelle indagini, ma soprattutto

come la noncuranza nel trattare il materiale informatico possa portare alla compromissione dell'intero processo a causa dell'invalidità delle prove raccolte. Tuttavia, sebbene conseguentemente ai grandi passi in avanti fatti inserendo queste norme nel nostro ordinamento giuridico abbiano prodotto risultati abbastanza soddisfacenti, il vero potenziale della computer forensics non è stato ancora espresso; ancor meno in Europa e nel Nostro Paese. Il progresso fornisce giorno per giorno nuove tecnologie al pari di tecniche innovative per la lotta al contrasto del crimine, non solo informatico. Lotta che quindi è sempre più possibile venga affrontata con approcci di maggiore efficacia e migliore efficienza. Non è distante da Noi il giorno in cui potremo garantire livelli di cyber security talmente alti da assicurare una quasi totale protezione, e quindi mitigare sensibilmente la criminalità in questo settore. A tal fine si auspica nella lungimiranza del legislatore italiano, che sappia cogliere questa tendenza di innovazione, e provveda di volta in volta in maniera confacente ai tempi.

BIBLIOGRAFIA

- G. Amato, V. Destito, G. Dezzani, C. Santoriello, *I reati informatici . nuova disciplina e tecniche processuali di accertamento*, Roma , Cedam, 2010;

- G. Costabile, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Ciberspazio e diritto*, 3, 2010;

- G. Ziccardi, *L'ingresso della computer forensic nel sistema processualpenalistico italiano: alcune considerazioni informatic- giuridiche, in L. Luparia, Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*, Giuffré, 2009;

- C. Jean, P. Savona, *Intelligence Economica. Il ciclo dell'informazione nell'era della globalizzazione*, Rubettino, 2011;

- A. Ghirardini, G. Faggioli, *Computer Forensics*, Apogeo, 2009;

- G. Conso, V. Grevi, M. Bargis, *Compendio di procedura penale*, CEDAM, 2014;

- F. Lisi, G. Muraro e A. Nuzzolo, *I reati informatici: nuova disciplina e tecniche processuali di accertamento*, Maggioli Editore, 2004;

- F. Casadei, A. Savoldi, P. Gubian, *"Forensics and SIM cards: an Overview"*, in *International Journal of Digital Evidence*, 2006, Volume 5, Issue 1;

- M.L. Di Bitonto, *L'accentramento investigativo delle indagini sui reati informatici, in Dir. dell'internet* , 2008, Ipsoa;

- M. Delle Donne, *Tecniche di indagine della Polizia Postale nell'ambito dei reati informatici e nella pedo-pornografia on-line*, in *Diritto&Diritti*, 2004;

- M. Epifani, *Analisi di telefoni cellulari in ambito giuridico,* in *Ciberspazio e Diritto*, 1, 2009;

- L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffrè, 2007;

- M. Daniele, *La prova digitale nel processo penale*, in *Rivista di diritto processuale* Anno LXVI (seconda serie) – n.2, 2011;

- O. Signorile, *Computer Forensic Guidelines: un approccio metodico – procedurale per l'acquisizione e analisi delle digital evidence*, in *Ciberspazio e Diritto,* Mucchi editore, 2009;

- F. Cajani, S.Aterno, *Aspetti giuridici comuni delle indagini informatiche,* in S.Aterno, F.Cajani, G. Costabile, M. Attiucci, G. Mazzaraco, *Computer forensic e indagini digitali*, Experta, 2011;

- S. Aterno e M. Mattiucci, *Cloud Forensics e nuove frontiere delle indagini informatiche nel processo penale,* in *Archivio Penale* fascicolo 3, 2013;

- A. Macrillo', *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. Internet*, 2008, Ipsoa;

- F. Bravo, *Indagini informatiche e acquisizione della prova nel processo penale*, in *Rivista di Criminologia, Vittimologia e Sicurezza* Vol. III - n. 3, Vol. IV – n. 1 – Settembre 2009–Aprile 2010;

- S. Battiato, F. Galvan, *La validità probatoria di immagini e video*, in *Sicurezza e Giustizia*, 2013;

- S. Battiato, F. Galvan, *verifica dell'attendibilità di un alibi costituito da immagini o video,* in *Sicurezza e Giustizia*,2013;

- Beyer, Stefanie, et al. "*Towards Fully Automated Digital Alibis with Social Interaction"*, in *Tenth Annual IFIP WG 11.9 International Conference on Digital Forensics*, 2014;

- H. Farid, M. Bravo, *"Image forensic analyses that elude the human visual system"*, in *SPIE Symposium on Electronic Imaging*, San Jose, CA, 2010;

- S. Battiato, G. Messina, R. Rizzo, "*Image Forensics. Contraffazione Digitale e Identificazione della Camera di Acquisizione: Status e Prospettive"* , Chapter in *IISFA Memberbook* ,2009;

- V. Calabrò, G. Costabile, S. Fratepietro, M. Ianulardo, G. Nicosia, "*L'alibi informatico. Aspetti tecnici e giuridici*", Chapter *in IISFA Memberbook*, 2010;

- L. Marafioti, *Digital evidence e processo penale*, in *Rivista Giuridica*, DeJure Giuffrè, 2011;

- E. Forlani, *La conservazione preventiva di dati informatici per l'accertamento di reati*, in *Dir. dell'Internet*, 2008, Ipsoa;

- A. Ester Ricci, *Digital evidence e irripetibilità delle operazioni acquisitive, in Dir. Proc. Pen.*, Giuffrè, 2010;

- L. Filippi, *Il rilevamento del "tracciato axe": una nuova denominazione per una vecchia tecnica d'indagine*, in *Giurisprudenza italiana*, 1999;

- M. Tonellotto, E*videnza informatica computer forensics e best practices*, in *Rivista di Criminologia, Vittimologia e Sicurezza* – Vol. VIII – n. 2 , 2014;

- S. Battiato, F. Galvan, *ricostruzione di informazioni 3d a partire da immagini bidimensionali*, in *Sicurezza e Giustizia*, 2013;

- F. Corona, *Network Analysis e Data Mining, nuove frontiere per l'intelligence tecnologica*, in *Gnosis rivista di Intelligence Italiana*, 2003;

- G. Ziccardi, "*l'utilità delle app legali*", in *Diritto24*, 2013;

- J. Shankar Babu, K. Sumathi, "*An Approach to Improve Computer Forensic Analysis via Document Clustering Algorithms*", in *International Journal of Innovative Research in Computer and Communication Engineering*, IJIRCEE, Vol. 2, Special Issue 4, settembre 2014;

- I. Riadi, *Log Analysis Techniques using Clustering in Network Forensics*, in *International Journal of Computer Science and Information Security*, IJCSIS, Vol. 10, n.7, luglio 2012;

- P. Myers, *Online Research Tools and Investigative Techniques*, in *Global Investigative Journalism Network*, 2015;

- G. Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, in *The Guardian*, 2013;

- P. Myers, *Data at Risk: How To Protect Your Sources and Your Work* , in *Global Investigative Journalism Network*, 2015 ;

- T. Dees, *3 great police iPhone apps*, in *PoliceOne.com*, 2011 ;

- M. Solomon, D. Barrett, N. Broom, *Computer Forensic Jumpstart*, Sibex, 2004;

- Chang-Tsun Li, *Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions*, Information Science Reference, 2010;

- C. L. T. Brown, *Computer evidence: Collection & Preservation*, Charles River media Inc., 2006;

- J. R. Vacca, *Computer Forensics: Computer Crime Scene Investigation. Second edition*, Charles River media Inc., 2005;

- P. Kanellis, E. Kiountouzis, N. Kolokotronis, D. Martakos, *Digital crime and Forensic science in Cyberspace*, Idea Group Publishing, 2006;

- E. Casey, *Handbook of computer crime investigation. Forensic tools and technology*, Acadamic Press, 2003;

- D. Schweitzer, *Incident Response: Computer Forensics Toolkit*, Wiley, 2003;

- D. Littlejohn Shinder, E. Tittel, *Scene of the Cybercrime. Computer Forensics Handbook*, Syngress, 2003;

- J. Dysart, *20 apps to help provide easier access to legal help, in American Bar Association Journal*, 2015;

- I. Charters, *The Evolution of Digital Forensics: Civilizing the Cyber Frontier*, CC, January 2009;

- E. Casey, *Digital Evidence and Computer Crime, Second Edition, Elsevier*, 2004;

- K. P. Chow, F. Law, Y.H. Mai, *Understanding Computer Forensics Requirements in China Via The "Panda Burning Incense" Virus Case*, in *Journal of Digital Forensics, Security and Law*, 2014;

- J. Liu, T. Uehara, *Computer Forensics in Japan: A Preliminary Study*, in *Availability, Reliability and Security, ARES '09 International Conference on*, 2009;

- A. Ariffin, J. Slay, H. Jazri, *Digital Forensics Institute in Malaysia: the way forward*, in *Digital Evidence and Electronic Signature Law Review* 9, 2012;

- J. Jordaan, *Ensuring the Legality of the Digital Forensics Process in South Africa*, in *International Journal of Computer Applications* (0975 – 8887) Volume 68 n.23, 2013;

- E.R. de Carvalho, *The Criminal Justice Response To Cybercrime*, in *140th International Training Course Participants'Papers*, 2008;

SITOGRAFIA

- http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf, NHCTU: association of chief police officers, The good practices guide for computer based electronic evidence, 2003;

- http://www.rfc-base.org/rfc-3227.html, Guidelines for evidence collection and archiving, 2002;

- Unità di Analisi sul crimine Informatico (Computer Crime Analysis Unit), dal sito www.poliziadistato.it;

- www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aise.html;

- http://ampedsoftware.com/it/;

- https://photosynth.net/;

- http://www.geocreepy.com/;

- http://www.softpedia.com/get/Internet/Other-Internet-Related/IntelliTamper.shtml;

- https://www.elevenpaths.com/labstools/foca/index.html#;

- http://www.geosetter.de/en/;

- http://spymasterproreview.com/;

- http://www.netan.go.kr/eng/index.do;
- http://www.cyanre.co.za/about/history/;

RIFERIMENTI GIURISPRUDENZIALI

- Cass. Pen. Sez. V, Sent. n. 6887 del 13 aprile 1999;

- Cass. Pen. Sez. VI, Sent. n.24617 del 24 febbraio 2015; (sequestro indiscriminato)

- Cass. Pen. Sez. V, Sent. n. 5337 del 16 marzo 1999; (Ammissione prove Documentali)

- Cass. Pen. Sez. IV, Sent. n. 3067 del 14 dicembre 1999;

- Cass. Pen. Sez. V, Sent. n. 31135 del 6 luglio 2007; (sistema e domicilio informatico)

- Cass. Pen. Sez. V, Sent. n. 46674 del 14 dicembre 2007; (sostituzione di persona)

- Cass. Pen. Sez. V, Sent. n.47096 del 14 dicembre2009; (posta elettronica)

- Cass. Pen. Sez. I, Sent. n.954 del 5 marzo 2009; (copia forense)

- Cass. Pen. Sez. I, Sent. n. 14511 del 5 marzo 2009; (valenza copia forense)

- Trib. di Roma Sez. V, Sent. n. 22205 del 20 novembre 2009; (ADSL wi-fi senza protezione)

- Cass. Pen. Sez. I, Sent. n. 25766, del 16 febbraio 2007;

- Trib. di riesame di Brescia Sez. II, Ordin. n. 11972 del 4 ottobre 2006;

- GUP di Vigevano , Sent. del 17 dicembre 2009; (gup Garlasco)

- Corte di Assise d' app. di Milano, Sez. I, Sent. n.55 del 17 dicembre 2014; (Rinvio Appello Garlasco)

- Cass. Pen. Sez. I, Sent. n. 44324 del 31 ottobre 2013; (caso Garlasco)

- Cass. Pen. Sez. V, Sent. n. del 11 dicembre 2015; (caso Garlasco)

- Cass. Pen. Sez. I, Sent. n. 264 del 26 febbraio 2014; (caso Cesaroni)

- Cass. Pen. Sez. I, Sent. n. 31456 del 21 maggio 2008; (caso Franzoni)

- Trib. Di Genova Sez. II, Ordin. n. 583 del 6 aprile 2004; (G8)

- Cass. Pen. Sez. V, Sent. n. 10309 del 18 ottobre 1993; (prove immagini)

- Cass. Pen. Sez. IV, Sent. n. 1344 del 13 dicembre 1995; (prove immagini)

-Trib. di Firenze Sez. II, Sent. n. 5675 del 8 gennaio 2015; (foto social)

- Supreme Court of NY, Einstein v. 357 LLC, 604199/07; (Corcoran Group)

RINGRAZIAMENTI

Il frutto di questo lavoro non mi sarebbe stato possibile senza il supporto di diverse persone. Esprimo, pertanto, la mia incondizionata stima ed ammirazione ad i miei relatori la Prof.ssa Barbara Sargenti e il Prof. Gianluigi Ciacci, per gli spunti di riflessione che mi hanno dato consentendomi di affrontare questo tema; ed alla Dott.ssa Serena Ianniello. Lei mi ha seguito durante tutto lo svolgimento della tesi con costanza e pazienza divenendo il mio punto di riferimento. Porgo, altresì, sentito riconoscimento e gratitudine al Maresciallo dei R.I.S. Paolo Martini presso l'I.S.T.I. dei Carabinieri di Velletri ed al Dott. Italo Trento Direttore Generale della Fondazione I.C.S.A., per avermi fornito diverso materiale interessante utilizzato all'interno dell'elaborato. Un pensiero d'amore, infine, va alla mia famiglia, in particolare ai miei genitori e a mia nonna che sono le assi portanti della mia vita e senza i quali non sarei nulla. Ed ancora un altro a Chiara e a Nicola, Pietropaolo, Alessia, che da sempre mi supportano, mi sono vicini e credono in me e in ogni azione che compio.

Grazie a tutti di vero cuore

Antonio Sapio

RIASSUNTO TESI

Il tema principale affrontato da questo elaborato è l'utilità della computer-forensics, la scienza in ambito giuridico che ruota attorno le diverse operazioni da compiere sul dato informatico ai fini di una valutazione come prova, all'interno di un processo penale. Viene svolto anche un attento esame delle principali e più recenti tecniche investigative relative all' "*informatic evidence*" con lo scopo di analizzare nello specifico le norme, le dinamiche e le applicazioni pratiche della computer forensics. La scelta di trattare tale argomento nasce dalla consapevolezza di come oggi il progresso tecnologico sia talmente integrato nella vita di tutti i giorni di ogni cittadino, e che abbia raggiunto livelli talmente alti, che non può essere ignorato dal diritto. Lo scopo sarà quello di comprendere e dimostrare quanto oggi delle procedure standarizzate siano necessarie ed incisive all'interno di un ordinamento giuridico, in special modo nell'ambito penale. La tesi è strutturata in quattro capitoli principali:

1) Introduzione alla computer forensics ;

2) La computer forensics nelle sue diverse fasi: dal reperimento della prova fino alla certificazione della sua validità;

3) Case study sulla ricerca delle prove;

4) La computer forensics nel prossimo futuro e negli altri Paesi più avanzati.

In primo luogo osserveremo come oggi le prassi e le principali linee guida siano inserite all'interno del sistema italiano; poi citeremo le recenti modifiche nel codice di procedura penale, indicando anche le principali istituzioni italiane che si avvalgono di queste procedure nelle loro mansioni. In questo primo capitolo, quindi, si vedrà l'apporto dato dalle tecniche di computer forensics che è stato sicuramente quello di permettere al nostro ordinamento, come anche a quelli esteri che le hanno adottate, di essere aggiornato ed all'avanguardia rispetto alle nuove contingenze. Ai nostri giorni non è pensabile che un sistema giuridico moderno sia privo di una legislazione adeguata sui reati informatici, considerata la crescita graduale e tendente al suo aggiustamento nell'ultimo decennio. Come non è

sostenibile che autorità competenti e professionisti del settore palesino carenze ad approcciarsi con protocolli pragmatici sia ai crimini canonici commessi mediante mezzi informatico-telematici ed ancor più alle nuove fattispecie emerse. Tutto ciò tenuto conto che i beni giuridici degni di tutela messi a rischio da questa tipologia di crimini sono di una certa rilevanza, ed hanno solitamente dinamiche che permettono di raggiungere una moltitudine di persone con estrema facilità ed in termini di tempo immediati.

Successivamente si approfondiranno le diverse fasi della computer forensics, iniziando dalle indagini fino ad arrivare al sequestro, alla certificazione e all'acquisizione in tribunale da parte dei giudici, soffermandoci anche sui principali dispositivi oggetto di esame, nonché le tecniche e gli strumenti più adottati nella prassi dagli inquirenti, con particolare attenzione ai più recenti. Difatti, Il più importante contributo dato dalla computer forensics è quello di rendere le indagini degli inquirenti più celeri e precise sotto vari aspetti, poiché gli elementi di prova che si rinvengono con questi mezzi sono molto dettagliati, ricchi di informazioni eterogenee e, se acquisiti correttamente, impossibili da confutare dal punto di vista della validità. Tutti fattori che si ripercuotono in modo indubitabile a beneficio dei tempi processuali, ovviamente qualora non vi siano nelle fasi di escussione e valutazione delle prove dubbi o incertezze sulle modalità d'acquisizione del materiale che viene presentato.

Di seguito verrà illustrato un "case study" sulle vicende dell'omicidio Garlasco ad opera di Alberto Stasi, ritenutosi questi un prezioso esempio riguardo la rilevanza ad utilizzare procedure standardizzate quando si rinviene del materiale informatico su una scena del crimine, con anche diversi collegamenti ad altri casi italiani simili. Da questa analisi emergerà chiaramente che trascurare queste prassi sia oltremodo dannoso e deleterio per un contenzioso. Una mancanza di accortezza come quella esaminata mostrerà perché sia facile perdere diversi elementi di prova che fin da subito avrebbero dato svolte significative nelle indagini, ma soprattutto come la noncuranza nel trattare il materiale informatico possa portare alla compromissione dell'intero processo a causa dell'invalidità delle prove raccolte.

Al termine effettueremo una panoramica delle principali innovazioni in campo tecnologico-investigativo che potrebbero essere introdotte in Italia in un prossimo futuro, cui seguirà una comparazione delle esperienze di computer forensics più significative negli ordinamenti sia delle nazioni che recentemente si stanno approcciando a questa disciplina, così come di quelle che ormai la praticano da tempo. Si evidenzierà nello specifico che il vero potenziale della computer forensics non è stato ancora espresso; soprattutto in Europa e nel Nostro Paese. Il progresso fornisce giorno per giorno nuove tecnologie al pari di tecniche innovative per la lotta al contrasto del crimine, non solo informatico. Lotta che quindi è sempre più possibile venga affrontata con approcci di maggiore efficacia e migliore efficienza. Non è distante da Noi il giorno in cui potremo garantire livelli di cyber security talmente alti da assicurare una quasi totale protezione, e quindi mitigare sensibilmente la criminalità in questo settore.

Nelle conclusioni verrà rassegnato un resoconto del nostro studio dove saranno nuovamente esposti in maniera consuntiva i risultati emersi dalle riflessioni affrontate in ciascun capitolo.