Stefano Aterno

Digital forensics (investigazioni informatiche)

Estratto da:

DIGESTO

delle Discipline Penalistiche

Aggiornamento

****

a cura di
Alfredo Gaito, Bartolomeo Romano,
Mauro Ronco e Giorgio Spangher

con la collaborazione di
Filippo Giunchedi, Antonella Mino e Ciro Santoriello

UTET
GIURIDICA

INDICE

Appello (evoluzione) di Daniela Chinnici . . . . . *p.* 1
Circolazione della prova e delle sentenze di Silvia Astarita . . . . . » 15
Codice antimafia di Antonio Balsamo . . . . . » 41
Collaborazione di giustizia di Alberto Cisterna . . . . . » 175
Decisione sul fatto incerto di Alfredo Bargi . . . . . » 209
Digital forensics (investigazioni informatiche) di Stefano Aterno . . . . . » 217
Femminicidio di Carmelo Domenico Leotta . . . . . » 248
Giudizio di rinvio di Marco Petrini . . . . . » 283
Giustizia penale differenziata di Mariangela Montagna . . . . . » 310
Igiene e sicurezza del lavoro (tutela penale) di Enrico Mario Ambrosetti . . . . . » 330
Manipolazioni del mercato di Maria Beatrice Magro . . . . . » 345
Misure cautelari personali di Giorgio Spangher . . . . . » 390
Obblighi internazionali in materia penale (convenzione Cedu) di Margherita Lombardo » 408
Organismo di Vigilanza (diritto penale) di Federico Romoli . . . . . » 422
Pirateria industriale (la disciplina penale della contraffazione del marchio e del brevetto dopo la legge n. 99/2009) di Annalisa Boido . . . . . » 448
Procedimento di prevenzione di Leonardo Filippi . . . . . » 466
Procedimento per la distruzione delle cose illegali di Mario Antinucci . . . . . » 512
Procedimento probatorio di Agostino De Caro . . . . . » 536
Processo agli enti di Giulio Garuti . . . . . » 556
Prova scientifica di Paola Felicioni . . . . . » 611
Regole di giudizio (dir. proc. pen.) di Filippo Raffaele Dinacci . . . . . » 644
Revisione di Tiziana Cavallaro . . . . . » 681
Verità reale e verità processuale di Oliviero Mazza . . . . . » 713

(52) La definizione è di CORDERO, *Procedura penale*, cit., 2012, 995, per il quale «La misura della probabilità sufficiente alla condanna non è codificabile».
(53) Tra i fautori della nuova regola, caldeggiata da sempre da STELLA, *Giustizia e modernità*, Milano, 2002, 151, va iscritto PALIERO, *Il ragionevole dubbio diventa criterio*, *GDir*, 2006, 73.
(54) Il dibattito, sulla nuova regola in esame, annovera numerosi interventi della dottrina, tra i quali, CAPRIOLI, *L'accertamento della responsabilità penale"oltre ogni ragionevole dubbio*, *CP*, 2009, 51; FERRUA, *La colpevolezza oltre ogni ragionevole dubbio*, in *Il nuovo regime delle impugnazioni tra Corte costituzionale e Sezioni Unite*, a cura di Filippi, Padova, 2007; IACOVIELLO, *Lo standard probatorio dell'al di là di ogni ragionevole dubbio e il suo controllo in Cassazione*, *CP*, 2006, 3857; CANZIO, *L'"oltre il ragionevole dubbio" come regola probatoria e di giudizio*, cit.
(55) Così, efficacemente CANZIO, *L'oltre il ragionevole dubbio*, cit., 306.
(56) Tale esigenza è sottolineata da IACOVIELLO, *Lo standard probatorio dell'al di là di ogni ragionevole dubbio e il suo controllo in Cassazione*, *CP*, 2007.
(57) Così CANZIO, *L'"oltre il ragionevole dubbio"*, cit., 306.
(58) In tali termini, PISANI, *Introduzione al processo penale*, cit., 70.
(59) Principio espresso da S.U., 10-7-2002, *GDir*, 38, 62, sviluppato anche da S.U., 29/30-10-2003, *GI*, 2004, 1230, con riguardo al controllo di attendibilità delle ipotesi antagoniste in relazione all'evidenza probatoria e ai criteri di verifica giudiziale della ricostruzione dei fatti
(60) Così, Cass. pen., sez. I, 24-10-2011, *CED*, 251507.
(61) Principio enunciato e sviluppato da TARUFFO, nel confronto con CANZIO E UBERTIS, in *Opinioni a confronto*, su *Fatto, Prova e Verità alla luce del principio dell'oltre il ragionevole dubbio*, in *Criminalia*, Pisa, 2009, 318.
(62) In tal senso TARUFFO, *op. ult. cit.*, 319.
(63) È emblematica in tal senso l'affermazione di Cass. pen., sez. II, 17-2-2009, (*FAmbr*, 2009, 1, 68), secondo cui «In materia di ricorso per cassazione, perché sia ravvisabile la manifesta illogicità della motivazione di cui all'art. 606, comma 1 lett. *e*) c.p.p., la ricostruzione contrastante con il procedimento argomentativo del giudice deve essere ovvia e inconfutabile, non rappresentare soltanto un'ipotesi alternativa a quella ritenuta in sentenza, in quanto la struttura logica dei ragionamenti è indipendente dalla verità degli enunciati che la compongono, mentre la proposta di una diversa lettura della documentazione in atti non è altro che la richiesta di un diverso giudizio di merito, inammissibile in sede di legittimità».

Digital forensics (investigazioni informatiche)

Bibliografia: APRILE, *Le indagini tecnico scientifiche: problematiche giuridiche sulla formazione della prova penale*, *CP*, 2003; ATERNO, *In materia di sequestro di HD e acquisizione della prova informatica: un caso eclatante*, *Dinternet*, 2005, n. 4, 365; ID., *Acquisizione e analisi della prova informatica*, *DPP*, 2008, n. 6, *Dossier* su *La prova scientifica nel processo penale*, a cura di P. Tonini; ID., *sub* art. 8, in AA.VV., *Cybercrime, responsabilità degli enti, prova digitale*, a cura di Corasaniti-Corrias Lucente, Padova, 2009; ATERNO-CAJANI-COSTABILE-MATTIUCCI-MAZZARACO, *Manuale di Computer Forensics*, Forlì, 2012; BITONTO-VITALE-MACRILLÒ-BARBIERI-FORLANI, *La ratifica della Convenzione del Consiglio d'Europa sul cybercrime: profili processuali*, *Dinternet*, 2008, 5, 503 ss.; CACCAVELLA, *Gli accertamenti tecnici in ambito informatico e telematico*, in ATERNO-MAZZOTTA, *La perizia e la consulenza tecnica*, Padova, 2006, 198; CAJANI, *Alla ricerca del log (perduto)*, *Dinternet*, Milano, 2007; CARNEVALE, *Copia e restituzione dei documenti informatici sequestrati: il problema dell'interesse ad impugnare*, *DPP*, 2009, 472; CASEY, *Digital evidence and Computer Crime*, *Academic Press*, 2000; CHIRIZZI, *Computer Forensics, il reperimento della fonte di prova informatica*, Roma, 2006; CISTERNA, *Tecniche di ricerca appropriate in base all'attuale quadro normativo*, *GDir*, 2009; COSTABILE-RASETTI, *Scena criminis, tracce informatiche e formazione della prova*, in *Cyberspazio e diritto*, IV, Modena, 2003; DI PIETRO-MANCINI, *A methodology for computer forensic analysis, Proceedings of the 3rd Annual IEEE information Assurance Workshop*, 2002, 41 ss.; DI PIETRO-ME, *Le investigazioni informatiche nel processo penale*, in *Tecnologie dell'informazione e comportamenti devianti*, L.e.d., Milano, 2004, 242; DIFFIE-HELLMAN, *New directions in cryptography*, *IEEE Transection on Information Theory*, novembre 1976; DUNI, *Le firme elettroniche nel diritto vigente*, *DII*, 200; LARONGA, *L'utilizzabilità probatoria del controllo a distanza eseguito con sistema satellitare g.p.s.*, *CP*, 2002, 3050; LUPARIA, *Le investigazioni informatiche in materia di pornografia minorile tra nuovi e vecchi abusi degli strumenti processuali*, *Dinternet*, 2005; ID., *Il caso "Vierika". Un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali*, *Dinternet*, 2006, n. 2, 155; ID., *La ratifica della convenzione sul cyber crime del Consiglio d'Europa. I profili processuali*, *DPP*, 2008; LUPARIA-ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007; MARAFIOTI, *Digital Evidence e processo penale*, *CP*, 2011, 4509; MARIOTTI-TACCONI, *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni voip*, *Dinternet*, 2008; MONTI, *La nuova disciplina del sequestro informatico*, in AA.VV., *Sistema penale e criminalità informatica*, Milano, 2009; PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, *DPP*, 2008, 700 ss.; RESTA, *La disciplina acquista maggiore organicità per rispondere alle esigenze applicative*, *GDir*, 2008; RIVEST-SHAMIR-ADLEMAN, *A method for obtaining Digital signature and public key cryptosystems*, in *Communications of the Acm*, XXI, febbraio 1978, 120 ss.; ID., *On digital signatures and public-key cryptosystems*, MIT *Laboratory for computer science*, *Technical Report*, *MIT/LCS/TR-212*, gennaio 1979; RUGGERI, *Profili processuali delle investigazioni informatiche*, in *Il diritto penale dell'informatica nell'epoca di Internet*, a cura di Picotti, Padova, 2004; SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, *GDir*, 2008; STRANO, *Relazione alla Conferenza sul Cybercrime*, Palermo, 3/5-10-2002; TONINI, *Documento informatico e giusto processo, DPP*, 2009, n. 4; ID., *Manuale di procedura penale*, Milano, 2011; VACIAGO, *I mezzi di ricerca della prova digitale nel procedimento penale e garanzie dell'indagato*, Torino, 2012; ZICCARDI, *Informatica e diritto penale: brevi note con particolare riferimento alla Rete Internet*, in *Il diritto nel cyberspazio*, Napoli, 1999.

Legislazione: artt. 244, 247, 248, 252, 254, 254 bis, 259, 260, 266, 266 bis, 352, 359, 360 c.p.p.; l. 18-3-2008, n. 48 (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); art. 163, f § 4, c.p.p. tedesco.

Sommario: 1. La digital forensics: concetto e definizione. Alterabilità e modificabilità del dato informatico e l'uso delle migliori tecniche per cristallizzare gli elementi di prova. – 2. Le norme del codice di procedura penale introdotte con la l. 18-3-2008 n. 48 (legge di ratifica della convenzione di Budapest 2001). – 3. (*Segue*). Sequestro e acquisizione di un sistema informatico e dei dati digitali. – 4. (*Segue*). Ispezione, perquisizione e acquisizione di un sistema informatico e telematico in funzione e non sequestrabile: banche dati complesse, servers e piattaforme di cloud computing. – 5. (*Segue*). L'accertamento tecnico urgente sui supporti informatici. – 6. (*Segue*). La custodia delle cose sequestrate ex art. 259 c.p.p. – 7. (*Segue*). Il sequestro di corrispondenza inoltrata per via telematica ex art. 254 c.p.p. – 8. (*Segue*). Il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni ex art. 254 bis c.p.p. – 9. Atti ripetibili e atti irripetibili. – 10. Strumenti investigativi informatici e mezzi di ricerca della prova atipici: il "pedinamento informatico" tramite sistema GPS. – 11. (*Segue*). L'appostamento informatico come mezzo di ricerca atipico della prova. – 12. (*Segue*). Il captatore informatico e la cosiddetta Remote Forensics: un trojan per la captazione occulta da remoto del contenuto di un sistema informatico.

1. *La digital forensics: concetto e definizione. Alterabilità e modificabilità del dato informatico e l'uso delle migliori tecniche per cristallizzare gli elementi di prova.*

L'acquisizione della prova digitale sta assumendo un'importanza vitale per la sorte di molte indagini (sia di polizia giudiziaria sia difensive) basate sull'acquisizione e sull'analisi di reperti informatici. Ciò non dipende soltanto dalla commissione di reati informatici propriamente detti o commessi ''a mezzo di sistemi informatici'' ma soprattutto dall'aumento di una capacità investigativa capace di sfruttare tutte quelle tecnologie in grado di scoprire ed acquisire le cosiddette digital evidence. Il cosiddetto ''alibi informatico'', che anni fa fece la sua prima apparizione in un'indagine contro le brigate rosse, oggi è tra gli alibi più difficili da demolire, ma anche da dimostrare con efficacia. Una buona conoscenza delle regole, delle metodologie e degli strumenti utili, consentono ad un buon forenser di scoprire e ''leggere'' i tanti segni lasciati dalla macchina sui supporti informatici. Ciò costituisce un indubbio vantaggio sia per la difesa sia per l'accusa.

La computer forensics è la disciplina che da tanti anni si occupa delle tecniche e degli strumenti utilizzati per recuperare gli elementi di prova (digitali) all'interno di un computer (1).

L'origine e l'evoluzione di questa scienza sono strettamente connesse all'evoluzione ed al progresso delle tecnologie dell'informazione e della comunicazione.

La definizione terminologica che vede l'utilizzo della ''s'' finale (che può apparire non corretto) risente dell'applicazione anglo americana e della letteratura che si riferisce a ''forensics sciences'' in cui il termine ''sciences'' è sottointeso e con il quale s'intende ''scienze forensi applicate al mondo del computer''. Nella letteratura italiana in alcuni casi si predilige il singolare, in altri ci si riporta alla tradizione anglo-americana (2).

Com'era inevitabile, contestualmente allo sviluppo tecnologico informatico su base industriale e commerciale, si è avuto un incremento di azioni e di condotte criminose basate sull'utilizzo di sofisticati strumenti telematici e di telecomunicazione.

L'utilizzo di strumenti informatici o telematici da parte della criminalità sia come strumento di offesa sia come obiettivo determina la presenza sulla scena criminis di numerosi elementi di prova digitale. Oltre ai tradizionali elementi di prova tipici del processo penale ''entrano'' nel processo, fin dalla fase delle indagini, ulteriori elementi di prova strettamente e inscindibilmente legati ad un sistema informatico o telematico e ugualmente idonei ad individuare un fatto o una circostanza utile all'accertamento della verità (3).

L'ambito di applicazione di questa scienza dipende in parte dall'oggetto delle sue attenzioni: vi è la computer forensics con riferimento all'analisi di dispositivi e supporti fisici e statici, la network forensics che ha come oggetto l'analisi forense di server e di reti, la mobile forensics che analizza i dispositivi cellulari e mobili.

Una volta recuperati, questi elementi di prova vengono analizzati, conservati, documentati e validati, attraverso tecniche di analisi forense testate a livello scientifico.

Uno dei massimi esperti di questa scienza, Casey, definisce le cosiddette digital evidence come «il complesso di informazioni digitali in grado di stabilire se un crimine è stato commesso o che possono rappresentare un collegamento tra un crimine e le sue vittime o i suoi esecutori» (4).

L'utilità delle tecniche di computer forensics in ambito processuale è emersa molto tempo fa soprattutto durante alcune indagini penali (molto anni prima della legge n. 48/2008 di cui parleremo nel prossimo paragrafo) come metodologia tecnica in grado di rinvenire tracce informatiche utilissime e fondamentali per le indagini (5). Da questo uso investigativo meramente utilitaristico, grazie anche alla dottrina anglosassone, si è passati ad un funzione di garanzia della digital forensics fino ad arrivare alla ripetibilità delle operazioni tecniche in tutti i casi in cui ciò è possibile. Prima delle modifiche normative arrivate solo nel 2008 questi accorgimenti tecnici e garantisti erano una rarità e negli anni che vanno dal 2000 al 2006 erano lasciati per lo più ad una preparazione occasionale e sporadica di qualche ufficiale di polizia giudiziaria appassionato o particolarmente specializzato. Solo negli anni successivi, con la maturazione delle competenze della Polizia postale e delle Telecomunicazioni si è avuta maggiore professionalità e un frequente ricorso a tali procedure.

Oggi gli elementi di prova digitale possono essere utili non soltanto in ambito penale ma anche nel processo civile e in quello amministrativo. Basti pensare all'importanza di che riveste l'acquisizione di elementi di prova digitali in tutti i settori che ruotano intorno alla responsabilità civile, alla responsabilità per danni derivante dalla circolazione stradale (oggi tutte le centraline delle automobili sono informatizzate e contengono dati preziosissimi), finanche alla responsabilità amministrativa, contabile e tributaria.

La crescente informatizzazione della società, la digitalizzazione della Pubblica Amministrazione e l'aumento del livello di sicurezza informatica e delle misure legate alla privacy dei dati e delle informazioni impongono uno sfruttamento sempre maggiore degli elementi di prova digitali e degli strumenti utili alla loro raccolta.

In un'indagine l'utilità e la genuinità di queste fonti

di prova investe tutti: sia la pubblica accusa, sia coloro che tendono a soluzioni difensive, sia coloro che sono chiamati a giudicare sull'ammissibilità di tali elementi e quindi poi devono dare una loro valutazione in sede decisionale.

Presupposto l'utilizzo di certi strumenti, la caratteristica fondamentale di queste tracce informatiche risiede nella certezza della loro esistenza ma al tempo stesso nella loro immaterialità e nella conseguente facile alterabilità.

Stiamo parlando di casi in cui lo strumento forense consente di recuperare dati cancellati in precedenza, di identificare l'intestatario di una linea dati o di un sito web, oppure quando consente all'investigatore di ricercare informazioni sul web (ad esempio, una fotografia dell'indagato oppure identificare un latitante che usa imprudentemente Facebook, Twitter o altri social network) oppure all'interno di grandi masse di dati.

Le evidenze digitali sono quelle fonti di prova memorizzate in qualsiasi tipo di strumento informatico come ad esempio gli smartphone, palmari, telefoni cellulari, server aziendali, postazioni di lavoro dei dipendenti, o altri sistemi cosiddetti informatici o telematici complessi (es. Cloud Computing). Questo tipo di evidenze sono caratterizzate da una ''carenza di materialità'' che porta ad una maggiore facilità di modifica accidentale durante la fase di acquisizione delle stesse. Si consideri ad esempio l'atto di aprire un documento di testo, che potrebbe essere utile alle indagini. La semplice apertura può essere sufficiente a modificare alcune caratteristiche del file. Affinché il dato non venga alterato è quindi necessario agire con la massima attenzione con l'ausilio di strumenti tecnici specifici e un alto rigore metodologico.

Si cercherà brevemente di spiegarlo con parole semplici.

Il dato informatico è costituito da una successione di 0 e di 1: paradossalmente, lo stesso dato informatico stampato su un foglio di carta è comunque una successione di 0 e di 1; questa serie di 0 e di 1 sono rappresentati dai simboli riprodotti sul supporto cartaceo utilizzando la codifica ASCII o altra codifica. La codifica in questione è una convezione che associa ad una precisa successione di 0 e di 1 un simbolo da riprodurre sul supporto cartaceo.

La parola ''ciao'' corrisponde ad una definita successione di zero e di 1: 01000100101001001010101111100101.

Sotto il profilo strettamente tipico del cosiddetto dato informatico è necessario considerare che i bit sono registrati su un dispositivo, il cui stato, impartendo opportuni comandi, può essere modificato da qualsiasi operatore che abbia accesso al sistema.

Nel caso di bit registrati su supporti non ri-scrivibili si può escludere a priori l'eventualità che tale dato possa essere stata modificato rispetto alla sua versione così come registrata sul supporto ma non può escludersi a priori che quel dato sia diverso dall'originario e che sia stato modificato prima di essere registrato (6).

Le digital evidence possono essere pertanto danneggiate o distrutte anche per colpa degli stessi investigatori, consulenti o periti non adeguatamente preparati che maldestramente maneggiano il supporto informatico.

È di tutta evidenza come questa eventualità può determinare il sorgere di problemi enormi sotto il profilo della genuinità della prova che poi si formerà in dibattimento.

Non esiste uno standard o una metodologia per il trattamento delle prove digitali forensi ma solo un insieme di procedure e strumenti più o meno consolidati e testati attraverso l'esperienza. Da anni la dottrina (7) si confronta sul tema affrontando il problema delle diverse metodologie da utilizzare nell'acquisizione e nell'analisi forense.

La fase acquisitiva della computer forensics consiste sostanzialmente in un'operazione di estrapolazione e riproduzione su idoneo supporto del dato digitale oggetto di indagine. L'operazione, nei limiti del possibile, deve svolgersi nella piena garanzia di integrità e non alterabilità delle tracce e nella prospettiva di una eventuale e successiva ripetibilità dell'operazione (magari in sede peritale).

Questa fase acquisitiva viene effettuata attraverso la bit-stream image (8), ovvero la realizzazione dell'''immagine'' bit a bit del contenuto del supporto posto sotto sequestro che consente di generare un hard disk praticamente identico all'originale: sia sotto il profilo logico sia sotto quello fisico; una acquisizione quindi condotta anche su tutte quelle parti ''vuote'' o presumibilmente tali che potrebbero assumere una importanza fondamentale ai fini delle indagini in quanto possono nascondere file o frammenti di file [slack (9)] cancellati.

Una volta eseguita l'acquisizione su tutti i supporti in sequestro è importante recuperare gli elementi informatici e tutte le informazioni utili alle indagini attraverso una ''analisi forense'' dei dispositivi digitali acquisiti.

È da sottolineare che questa analisi deve essere compiuta con metodi che consentano di conservare, documentare, validare e interpretare le informazioni o gli elementi di prova che derivano dalle tracce digitali presenti in quella che è stata chiamata, molto efficacemente, scena criminis, rinvenuta all'interno del sistema o del supporto informatico (10). Per tali operazioni si ricorre ad idonei strumenti hardware e software in commercio o comunque utilizzati dalle forze di polizia, militari e agenzie governative di ogni parte del mondo, molti dei quali ''proprietari'' e altri open source.

Innanzitutto il sistema di acquisizione e di analisi dovrà operare con l'ausilio di un blocco di scrittura che consente di non compromettere i dati escludendo qualsiasi trattamento, variazione, aggiunta, cancellazione (soprattutto colposa) sul supporto originale. Nella formazione dell'"immagine" dovrà essere creata anche una cosiddetta "impronta" che deve contraddistinguere univocamente la traccia dell'analisi forense e che garantisce l'integrità del dato. Tale operazione si chiama hashing a chiave simmetrica, con algoritmo di classe MD5 e che genera un'impronta della lunghezza di 128 bit (16 byte) (11). Questa impronta costituisce un riferimento certo alla traccia originale e non ne consente la ricostruzione.

L'eventuale volatilità del dato informatico e la sua modificabilità nel tempo determinano l'inequivocabile inattendibilità di un reperto informatico male acquisito, mal conservato e mal analizzato. In queste ipotesi una eventuale ripetizione della procedura di hashing sul supporto produrrà un algoritmo diverso che rileverà una modifica del supporto rispetto all'originale.

Se durante l'operazione viene compromessa la genuinità e l'integrità dei dati contenuti sui supporti il risultato sarà l'inattendibilità e la possibile inutilizzabilità degli elementi probatori raccolti con un probabile pregiudizio per una delle due parti processuali.

Oggi è di tutta evidenza che la ricerca e l'analisi della prova digitale deve interessare anche la difesa degli indagati in relazione ad indagini difensive "informatiche" volte a confutare ipotesi accusatorie o ricercare prove per utili e fondati "alibi informatici" (12).

L'integrità della prova digitale fino al dibattimento è pertanto un fattore che deve interessare tutte le parti processuali come del resto, deve interessare le stesse parti, anche il procedimento per il suo corretto trattamento e custodia. Come segnalano alcuni autori (13), deve essere dedicata massima cura alla catena di custodia (chain of custody) ovvero alla metodologia di custodia e di trasporto, sia fisico sia virtuale delle digital evidences. Questa procedura è finalizzata a consentire la tracciabilità e ripetibilità dell'acquisizione e dell'analisi degli elementi di prova digitali in qualsiasi fase del processo.

Entrando nel merito, per dimostrare la non ripudiabilità del reperto prodotto in giudizio e quindi la sua validità e utilizzabilità probatoria, bisogna innanzi tutto illustrare le modalità con cui è stato trattato.

Più in generale, il processo di computer forensics prevede l'esecuzione delle seguenti fasi:

a) riconoscimento e identificazione della fonte di prova;

b) acquisizione del dato (o del sistema);

c) conservazione e protezione del dato (o del sistema), trasversale rispetto a tutte le successive fasi;

d) analisi forense;

e) valutazione dei risultati estratti dall'analisi (sotto il profilo tecnico, giuridico ed investigativo);

f) presentazione dei risultati (al titolare delle indagini, al Giudice o al committente in caso di attività difensiva o stragiudiziale).

Tali macro-attività rappresentano il ciclo di vita del dato nell'ambito dell'analisi forense dal momento della sua identificazione fino alla chiusura delle attività.

Quest'ultime devono essere sempre affiancate dalla redazione della documentazione sulla catena di custodia e di verbali nei quali devono essere riportate dettagliatamente tutte le attività svolte soprattutto in termini di conservazione e protezione del dato.

L'individuazione del reperto informatico è un'operazione importante. Se il reperto non viene prontamente individuato, si espone per un tempo maggiore al rischio di inquinamento e alle volte alla sua distruzione o dispersione.

L'individuazione del reperto informatico deve essere esaustiva ed approfondita, non potendo riguardare solo supporti tipicamente "informatici", bensì anche altri tipi di supporto che potrebbero contenere tracce informatiche non a prima vista evidenti.

Ulteriore aspetto da considerare in questa fase è la corretta conservazione e imballaggio del supporto su cui sono registrati i reperti.

In base alla tipologia del reperto andranno accuratamente scelte gli opportuni contenitori e anche le modalità di conservazione.

La fase di acquisizione del reperto informatico è la più delicata e complessa in assoluto. La caratteristica essenziale consiste nella completezza delle operazioni ovvero non solo nell'acquisizione di tutti i bit dei supporti rinvenuti ma anche nella corretta individuazione dei reperti informatici e nella loro accurata documentazione al fine di garantire il rispetto dei principi sopra enunciati.

L'attività svolta in fase di acquisizione infatti deve essere accuratamente documentata, possibilmente utilizzando dispositivi che registrino automaticamente quanto viene eseguito. In questo modo, infatti, si conserva traccia di tutte le operazioni compiute, atteso che, in questi casi per praticità, vengono solitamente sintetizzate le attività poste in essere, ma non si descrivono in maniera dettagliata i singoli comandi battuti.

Attraverso strumenti software dedicati si possono analizzare i file contenuti su un supporto sotto tutti i profili e valutare le moltissime informazioni che essi possono fornire. Questi software sono in grado di analizzare anche file cancellati o parte di file residuati nella memoria di un hard disk o di un supporto; è di tutta evidenza la grande utilità di tale funzione per le indagini sia dell'accusa sia della difesa.

Durante la fase di analisi del reperto bisogna evitare

di alterare il supporto che definiamo ''sorgente''. Pertanto particolare attenzione dovrà essere mostrata eseguendo tutte le operazioni di analisi su una o più copie dello stesso.
Una caratteristica fondamentale della fase di analisi è la riproducibilità delle operazioni eseguite, nel senso che eseguendo operazioni identiche bisogna ottenere sempre lo stesso risultato.
Questa caratteristica garantisce che, nella dialettica del processo, qualsiasi rilievo sollevato da una parte in merito ad un reperto informatico possa essere verificato anche dalle altre parti e le eventuali criticità sottoposte eventualmente a contraddittorio.
Visto che il reperto informatico può subire alterazioni, inquinamenti, contraffazioni, occorre accertare se si siano verificati questi eventi, se essi erano potenzialmente verificabili, e chi avrebbe eventualmente potuto compiere tali operazioni.
Infine si arriva alla fase finale della presentazione delle conclusioni: è il momento in cui il consulente tecnico trasmette le conclusioni della propria attività di accertamento tecnico al pubblico ministero, al difensore o, se perito, al giudice. Quindi se la presentazione dei risultati non ottiene il risultato sperato di trasmettere a tutti gli interlocutori i fatti accertati con la chiarezza necessaria, l'intero lavoro rischierà di essere vanificato (14).
Relativamente allo stato di funzionamento dei sistemi oggetto di analisi, una delle classificazioni più importanti è la seguente:
– analisi cosiddetta post-mortem: quando ci si riferisce ad una analisi effettuata a macchina spenta ed eseguita dopo la consumazione di un illecito. Questo tipo di attività è la più sovente nelle azioni di polizia giudiziaria, quando ad esempio si sequestra un hard disk o altra memoria da analizzare, successivamente, in laboratorio (o presso un consulente tecnico).
– live forensics analisys: consistente in tecniche di analisi su sistemi attivi sviluppate negli ultimi anni soprattutto in ipotesi di sistemi informatici complessi, in presenza di un grande numero di server che non possono essere spenti e come vedremo in caso di cloud computing.
Il trattamento di reperti informatici si suddivide, essenzialmente, in due grosse categorie: la Disk Forensics e la Network Forensics.
La Disk Forensics si occupa dell'acquisizione e dell'analisi dei reperti informatici presenti sui supporti fisici, come dischi rigidi, floppy disk, cd-rom, pen drive, ecc., oltre ai sistemi così detti embedded (15), che possono comunque assolvere alla funzione di supporto su cui registrare i dati. Altresì rientra nella Disk Forensics il trattamento dei reperti informatici presenti all'interno di palmari, macchine fotografiche digitali, smart card e telefoni cellulari.
La Network Forensics, invece, si occupa dell'acquisizione e dell'analisi dei reperti informatici trasmessi attraverso una rete di trasmissione dati fra computer, nonché dell'acquisizione ed analisi dei dati che sono effetto di eventi verificatisi in una rete di trasmissione dati.
Poiché esistono dispositivi che, pur avendo la dimensione di un accendino, possono contenere centinaia di mega byte, per procedere in modo corretto nella fase di acquisizione del reperto, occorre individuare le caratteristiche tecnologiche del supporto stesso.
Un disco rigido è costituito al suo interno da alcuni dischi di rame e da uno o più ''braccia'' che si spostano lungo tutto il raggio del disco. In seguito, il disco viene suddiviso in unità minime chiamate settori, che, di solito, sono grandi 512 byte; tuttavia, poiché spesso il sistema operativo non può indirizzare tutti i settori definiti sul disco, si raggruppano settori successivi logicamente fra loro in modo da costituire un cluster (16).
Il cluster, quindi, può essere definito l'unità minima indirizzabile sul disco.
Altri elementi del disco rigido che sono oggetto dell'analisi forense sono i file, la tabella di allocazione dei file stessi e la ''partizione'' dei dischi (17). Tuttavia, mentre questi ultimi sono i classici elementi con i quali si confronta un tecnico informatico, particolare rilevanza nella Disk Forensics la assume lo slack (18).
Per cercare di far comprendere cosa sia uno slack, possiamo immaginare il file come se fosse una video cassetta, se registriamo sulla stessa video cassetta prima un file di 2 ore e successivamente sempre sulla stessa video cassetta un film di un'ora e 45 minuti (ripartendo dall'inizio del nastro), possiamo facilmente verificare che gli ultimi 15 minuti del precedente film siano ancora visibili. Ebbene questi 15 minuti del film precedente sono lo ''slack'' di questa video cassetta.
Attraverso questi sistemi di forensics è possibile recuperare anche i file cancellati e a volte anche cancellati abbastanza bene.
Quando il sistema operativo esegue la cancellazione logica di un archivio, questo non viene distrutto o cancellato completamente, in quanto il sistema operativo provvede solo a rendere disponibile lo spazio sul disco precedentemente occupato dal file.
Ma il file appunto non viene cancellato. Possiamo dire che ''si sposta'' e fa posto al nuovo file.
Quando l'utente esegue la cancellazione di un file, il sistema operativo provvede solo ad annotare la disponibilità di uno spazio fino a quel momento occupato e che è diventato disponibile per nuove registrazioni, con la conseguenza che, fino al momento di riutilizzo degli stessi settori precedentemente impiegati, sarà possibile recuperare frammenti dei file cancellati ed, in alcuni casi, anche l'intero file.

Infatti, sino a che il sistema non ''scrive'' un nuovo file sopra lo stesso piccolissimo settore del vecchio, il file originario non verrà mai cancellato. È ben possibile però ad esempio che se ne cancelli anche solo una parte.

Nello specifico invece la network forensics si occupa dell'esame e correlazione dei file di log di uno o più sistemi, cioè dell'analisi del registro degli eventi che sono accaduti all'interno di un sistema (Log) (19).

Si occupa inoltre della comparazione del registro di log di un sistema fra quello di altri sistemi al fine di stabilire una successione di eventi che si è verificata all'interno di una rete di computer (si pensi alle reti aziendali complesse); ad esempio per ogni messaggio di posta elettronica inviato da un server SMTP (20), deve risultare un evento di ricezione del messaggio per ciascun server ricevente.

Queste tipologie di informazioni molte volte risultano determinanti in quanto costituiscono tracce memorizzate dai sistemi infrastrutturali (in particolar modo nella c.d. network forensics aziendale).

Tipicamente le informazioni di questo tipo sono da ricercarsi su elementi quali ad esempio:

– Firewall;
– Intrusion Prevention Systems;
– Proxy di navigazione;
– Domain Controller;
– Server di Posta;
– Sistemi di Identity Management;
– Server Applicativi (SAP, CRM, Custom, ecc.).

Più sono gli elementi tecnologici in grado di produrre tracce e maggiori sono le relative fonti di informazione. Per questo motivo appare di fondamentale importanza scegliere oculatamente le fonti d'informazione da cui estrarre i dati ma soprattutto essere capaci ad estrarle (21).

(1) Per tutti, E. Casey, *Digital evidence and Computer Crime*, *Academic Press*, 2000.

(2) Per una esauriente analisi delle origini e dell'uso del termine forensic, si veda, Costabile-Rasetti, *Scena criminis*, *tracce informatiche e formazione della prova*, in *Cyberspazio e diritto*, IV, Modena, 2003, n. 3/4, 273; Luparia-Ziccardi, *Investigazione penale e tecnologia informatica*, Milano, 2007, 3 ss. Aterno, *Acquisizione e analisi della prova informatica*, *DPP*, 2008, n. 6, Dossier su *La prova scientifica nel processo penale*, a cura di P. Tonini. Si confronti anche, Vaciago, *I mezzi di ricerca della prova digitale nel procedimento penale e garanzie dell'indagato*, Torino, 2012.

(3) P. Tonini, *Documento informatico e giusto processo*, *DPP*, 2009, n. 4.

(4) E. Casey, *Digital evidence*, cit., 196.

(5) Per un primo caso di alibi informatico basato su circostanze e riscontri ricavati dai dati di un personal computer, grazie ai quali all'indagato è stata revocata la misura della custodia cautelare, si veda, ordinanza G.I.P. T. Roma, 27-5-2000, inedita, relativa alla scarcerazione di un ragazzo sospettato di essere l'autore delle telefonate di rivendicazione dell'omicidio del prof. D'Antona ucciso dalle Brigate Rosse.

(6) Si veda, Cass. pen., sez. I, 25-2-2009, n. 11503, *CED*, 243495, nel punto in cui afferma in tema di onere probatorio che è anche colui che contesta l'eventuale irripetibilità dell'accertamento che deve comprovare forme di distruzione o alterazione dei dati acquisiti tali da confortare il proprio assunto e non limitarsi a prospettare ipotetiche situazioni potenziali che esulano dalla fattispecie sottoposta all'esame della Corte.

(7) Per i primi e pregevoli contributi della dottrina italiana si vedano, Costabile-Rasetti, *Scena criminis*, *tracce informatiche e formazione della prova*, cit., 273; Di Pietro-Me, *Le investigazioni informatiche nel processo penale*, in *Tecnologie dell'informazione e comportamenti devianti*, Milano, 2004, 242; L. Luparia, *Le investigazioni informatiche in materia di pornografia minorile tra nuovi e vecchi abusi degli strumenti processuali*, *Dinternet*, 2005, n. 5, 484; F. Ruggeri, *Profili processuali delle investigazioni informatiche*, in *Il diritto penale dell'informatica nell'epoca di Internet*, a cura di Picotti, Padova, 2004, 153 ss.; si consenta il rinvio a S. Aterno, *In materia di sequestro di HD e acquisizione della prova informatica: un caso eclatante*, *Dinternet*, 2005, n. 4, 365; L. Luparia, *Il caso ''Vierika''. Un'interessante pronuncia in materia di virus informatici e prova penale digitale. I profili processuali*, *Dinternet*, 2006, n. 2, 155; Di Pietro-Mancini, *A methodology for computer forensic analysis*, Proceedings of the 3rd Annual IEEE information Assurance Workshop, 2002, 41 ss.

(8) La bit stream image è una sorta di ''clonazione'' del supporto informatico sotto sequestro che determina una ''immagine'' del contenuto del HD su altro supporto preparato all'occorrenza. Sulla fase dell'acquisizione delle tracce informatiche ovvero bitstream image, si vedano, Di Pietro-Me, L*e investigazioni informatiche nel processo penale*, cit., 251; Costabile-Rasetti, *Scena criminis*, *tracce informatiche e formazione della prova*, cit., 283.

(9) Slack sono una porzione di quel che rimane di un file quando viene cancellato superficialmente e sopra il quale in parte il sistema informatico stesso riscrive (vedi avanti).

(10) Costabile-Rasetti, *Scena criminis, tracce informatiche e formazione della prova*, cit., 275. Per il concetto informatico di scena criminis informatica si veda anche M. Strano, *Relazione* alla Conferenza sul Cybercrime, Palermo, 3/5-10-2002.

(11) In materia di algoritmi e chiavi asimmetriche, si vedano, Diffie-Hellman, *New directions in cryptography*, in *IEEE Transection on Information Theory*, novembre 1976. Per una esauriente e competente analisi anche da un punto di vista storico, si veda per tutti, Duni, *Le firme elettroniche nel diritto vigente*, *DII*, 2006, 501 ss. Rivest-Shamir-Adleman, *On digital signatures and public-key cryptosystems*, MIT *Laboratory for computer science*, *Technical Report*, *MIT/LCS/TR-212*, gennaio 1979; Id., *A method for obtaining Digital signature and public key cryptosystems*, in *Communications of the Acm*, XI, febbraio 1978, 120 ss.

(12) Per un primo caso di alibi informatico basato su circostanze e riscontri ricavati dai dati di un personal computer, grazie ai quali all'indagato è stata revocata la misura della custodia cautelare, si veda, G.I.P. T. Roma, 27-5-2000, inedita.

(13) Di Pietro-Me, *Le investigazioni informatiche nel processo penale*, cit., 251; Costabile-Rasetti, *Scena criminis*, *tracce informatiche e formazione della prova*, cit., 278; A. Monti, *Prime impressioni sul rapporto della ''Commissione Meo'' – http://www.interlex.it/pa/amonti65.htm*; G. Ziccardi, *Informatica e diritto penale: brevi note con particolare riferimento alla Rete Internet*, in *Il diritto nel cyberspazio*, Napoli, 1999; L. Chirizzi, *Computer Forensics, il reperimento della fonte di prova informatica*, Roma, 2006.

(14) E.D. Caccavella, *Gli accertamenti tecnici in ambito informatico e telematico*, in Aterno-Mazzotta, *La perizia e la consulenza tecnica*, Padova, 2006, 198.

(15) Si chiamano embedded sistemi non necessariamente basati su dati digitali; es. telecamere di vecchio tipo a circuito chiuso.

(16) E.D. Caccavella, *Gli accertamenti tecnici in ambito informatico e telematico*, cit., 199 ss.

(17) Si chiama partizione di un disco una sua parte interna che per qualche motivo potrebbe essere separata dal resto della memoria del disco creando uno spazio informatico all'interno del disco stesso. A volte le partizioni possono essere in uso a soggetti diversi ma tutti fruitori dello stesso Personal computer. Le partizioni sono accessibili con password diverse.
(18) Lo slack è frammento di file. Se un file si cancella tramite sovrascrittura è possibile che un frammento, lo slack appunto non si cancelli e rimanga in qualche angolo del PC fino a che anch'esso non verrà sovrascritto e quindi cancellato definitivamente per sempre.
(19). Nella lingua inglese il termine log indica il diario di bordo di una nave, ma viene applicato estensivamente anche al computer. Nel gergo informatico, "loggare" (da verbo inglese to log) significa registrare all'esito di una attività di monitoraggio; pertanto il log file (o file di log) è il risultato di tale operazione, che assume la forma di un file (di testo) nel quale vengono appunto indicate le operazioni che l'utente compie durante la sua sessione di lavoro. Per un tentativo di definizione si veda F. CAJANI, in *Alla ricerca del log (perduto)*, commento a T. Chieti, 30-5-2006, n. 139, *Dinternet*, Milano, 2007.
(20) *Simple Mail Transfer Protocol (SMTP)*: è lo standard per la trasmissione di posta elettronica su Internet. Un server SMTP riceve i messaggi destinati a tutti gli utenti di un dominio Internet, inviatigli da un client SMTP (p.e. Outlook Express). È un protocollo da server a server.
(21) Per un'analisi tecnica delle 10 regole d'oro della computer forensics e i 7 comportamenti da evitare, si veda ATERNO-CAJANI-COSTABILE-MATTIUCCI-MAZZARACO, *Manuale di Computer Forensics*, Forlì, 2012, 21.

2. *Le norme del codice di procedura penale introdotte con la l. 18-3-2008, n. 48 (legge di ratifica della convenzione di Budapest 2001).*

La l. 18-3-2008, n. 48 ha ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2001, introducendo per la prima volta in Italia una disciplina specifica in tema di acquisizione degli elementi di prova digitali grazie alla modifica degli articoli in materia di perquisizione, sequestro, acquisizione e conservazione dei dati presenti su supporti informatici (22).

La Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001 è stato il primo accordo internazionale riguardante i crimini commessi attraverso internet e le altre reti informatiche. La necessità di questa legislazione è emersa fin dal 1995 con la "raccomandazione n. 13" del Consiglio d'Europa dove per la prima volta è stato posto l'accento non solo sui problemi di diritto sostanziale e processuale connessi all'informazione tecnologica ma soprattutto al necessario coordinamento investigativo tra gli Stati sottoscrittori.

La Convenzione contiene alcune norme che disciplinano in generale la classica area dei cybercrime, ma soprattutto una serie di disposizioni importanti sull'acquisizione, sulla raccolta e sulla conservazione delle cosiddette digital evidence. La Convenzione aveva lo scopo di suggerire e indirizzare una politica comune fra gli stati aderenti suggerendo una legislazione che fosse realmente in grado di combattere il crimine informatico in maniera coordinata ed efficace. Essa è il risultato di un lavoro condotto per quattro anni da un Comitato di esperti del Consiglio d'Europa costituito ad hoc, al quale hanno dato il proprio contributo anche alcuni Paesi non appartenenti al Consiglio quali gli Stati Uniti, il Canada e il Giappone. Alla data del 1º novembre 2012 la Convenzione è stata firmata, ratificata ed è in vigore soltanto in 36 Stati rispetto ai 51 Paesi firmatari della Convenzione.

In Italia l'iter parlamentare di ratifica è iniziato l'11 maggio 2007 quando il Consiglio dei Ministri ha approvato lo schema di disegno di legge recante l'autorizzazione alla ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica (sottoscritta a Budapest il 23-11-2001), la sua esecuzione nonché le norme di adeguamento dell'ordinamento interno.

Il successivo 19 giugno 2007 il Governo ha presentato l'atto al Parlamento che in un periodo di cinque mesi ha discusso il testo in Commissione ascoltando anche il parere di alcuni tra i maggiori esperti del settore (investigatori, forze dell'ordine e studiosi della materia e della computer forensics). Il Governo però nel febbraio/marzo 2008 non ha più la fiducia delle Camere ed è costretto a dimettersi. Nell'ultima assemblea parlamentare della Camera, il 20 febbraio 2008, con alcune modifiche apportate frettolosamente nel corso del breve dibattito in aula, l'atto del Governo viene approvato dalla Camera con alcuni importanti emendamenti maturati già in occasione dei lavori in Commissione (23).

Pochi giorni dopo, l'atto giunge al Senato della Repubblica e il giorno stesso in cui la 3ª Commissione Senato (27 febbraio 2008) lo esamina per la prima volta, viene portato in aula parlamentare e approvato (24).

La l. 18-3-2008, n. 48 così approvata è stata pubblicata il 4 aprile del 2008 sulla Gazzetta Ufficiale ed è entrata in vigore il giorno seguente ovvero il 5 aprile 2008.

Sulla data di entrata in vigore, c'è stata una qualche incertezza in seguito ad una sentenza del Tribunale del Riesame di Roma (25) che ha ritenuto di fissare l'entrata in vigore della norma il primo ottobre dello stesso anno. Il Tribunale romano, investito tra le altre cose anche di una questione riguardante la violazione dell'art. 254 bis c.p.p. ha stabilito che le eccezioni dedotte dalla difesa dell'indagato non potevano essere apprezzate, perché si fondavano su una norma, appunto l'art. 254 bis c.p.p., che non risultava in quel momento in vigore. Secondo il Tribunale la normativa vincolava lo Stato italiano non il giorno dopo la pubblicazione sulla Gazzetta Ufficiale (5 aprile 2008) ma a partire da tre mesi dopo il deposito al Consiglio d'Europa della legge di ratifica, termine

che coincideva appunto con il 1º ottobre 2008 (26). La sentenza faceva riferimento per la decorrenza dei termini al deposito che doveva avvenire (dopo la firma del Presidente della Repubblica) presso il Segretario Generale del Consiglio d'Europa.

Sul punto, a seguito del ricorso della difesa, è intervenuta la Suprema Corte di Cassazione (27) che ha infatti chiarito che la legge n. 48 è entrata in vigore il 5 aprile del 2008 e non il primo ottobre dello stesso anno.

A ben vedere e come affermato dalla Suprema Corte, ai sensi dell'art. 36 delle disposizioni della Convenzione e delle norme comunitarie, la procedura indicata dal tribunale romano riguarda l'efficacia della convenzione nei confronti degli stati membri per gli obblighi assunti tra stati e non invece l'entrata in vigore di norme processuali interne di uno stato sovrano.

Le norme introdotte dalla legge n. 48/2008 e le modifiche apportate al codice di procedura penale sono importanti proprio per quelle esigenze di immodificabilità delle digital evidence e di genuinità degli elementi di prova a cui si è fatto riferimento nel par. 3. anche e soprattutto in considerazione dell'assenza di riferimenti di garanzia nel testo uscito dal Governo.

In tema di ispezioni informatiche, con le modifiche aggiuntive all'art. 244 c.p.p., si è stabilito che l'autorità giudiziaria possa disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. Sotto il profilo della perquisizione cosiddetta informatica, invece, la modifica ha interessato l'art. 247 c.p.p. al quale è stato aggiunto un nuovo co. 1 bis, il quale stabilisce che ove si ha motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, deve esserne disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Se riflettiamo sulla circostanza che sia l'art. 244 c.p.p. sia l'art. 247 c.p.p. nella stesura originaria giunta direttamente nell'aula parlamentare prevedevano soltanto la possibilità che dati e sistemi informatici potessero essere ''perquisiti'' senza indicare ''in che modo'', si comprende come, con un emendamento di fondamentale importanza e lungimiranza, l'introduzione della disposizione «adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione» abbia assunto un rilievo fondamentale e determinante.

Tale disposizione racchiude il principio alla base delle modifiche e del senso della normativa in questione proprio in virtù della preoccupazione ''degli esperti'' e poi del legislatore dell'aula di fornire una garanzia di genuinità alle prove che emergono da dati o sistemi informatici oggetto di ispezioni o perquisizioni (28) (si veda al par. 3. l'analisi approfondita delle norme citate).

Con la legge di ratifica della Convenzione di Budapest è stata altresì prevista la modifica dell'art. 254 c.p.p. in materia di sequestro di corrispondenza e si è inserito l'art. 254 bis c.p.p. relativo alla possibilità di sequestrare dati informatici presso i fornitori di servizi informatici, telematici e di telecomunicazioni (v. *infra*, par. 5. e 8.); è stata inserita inoltre una disposizione sul problema che concerne la custodia delle cose sequestrate (art. 259, 2º co., c.p.p.) e alcune garanzie circa il sequestro e la custodia di cose deperibili come appunto i dati informatici (modifica dell'art. 260, 2º co., c.p.p.).

Per i casi di urgenza è stata altresì prevista una modifica all'art. 352 c.p.p. in materia di perquisizioni. In tutte le ipotesi di flagranza del reato, ovvero nei casi di cui al 2º co. dello stesso articolo, quando sussistono i presupposti e le altre condizioni previste, gli ufficiali di polizia giudiziaria possono adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione e procedere altresì alla perquisizione di sistemi informatici o telematici 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 cancellate o disperse.

L'art. 9, 3º co., legge n. 48/2008 ha integrato il 2º co. dell'art. 354 c.p.p., estendendo il potere della polizia giudiziaria di compiere accertamenti urgenti, finalizzati a conservare tracce e cose pertinenti al reato o ad evitare l'alterazione di luoghi e cose, ai dati, alle informazioni, ai programmi informatici e ai sistemi informatici o telematici. La norma prevede che gli ufficiali di polizia giudiziaria adottino le misure tecniche o impartiscano le prescrizioni necessarie ad assicurare la conservazione dei dati, delle informazioni e dei programmi oggetto di accertamento, nonché ad impedirne l'alterazione e l'accesso. Ciò, prosegue la norma, può essere effettuato ove possibile, attraverso la loro duplicazione mediante una procedura tale da assicurare la conformità della copia all'originale e la sua immodificabilità.

La legge n. 48/2008 ha novellato infine anche l'art. 248 c.p.p. (richiesta di consegna di dati, informazioni e programmi informatici) in quanto il Legislatore ha stabilito che, al fine di evitare di compiere atti particolarmente invasivi della sfera delle persone, l'Autorità Giudiziaria può invitare il possessore a consegnare anche tali dati informatici invece di procedere alla perquisizione.

(22) Per i primi commenti in generale sulla legge n. 48/2008 cfr. ATERNO-CUNIBERTI-GALLUS-MICOZZI, *Commento alla legge di ratifica della convenzione di Budapest del 23 novembre 2001*, in *http://www.giuristitelematici.it/uploads/commento-budapest.pdf* maggio 2008; per un commento articolo per articolo cfr., BITONTO-VITALE-MACRILLÒ-BARBIERI-FORLANI, *La ratifica della Convenzione del Consiglio d'Europa sul cybercrime: profili processuali*, *Dinternet*, 2008, 5, 503 ss.; L. LUPARIA, *La ratifica della convenzione sul cyber crime del Consiglio d'Europa. I profili processuali*, *DPP*, 2008, 717 ss.; L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, *DPP*, 2008, 700 ss.; G. RESTA, *La disciplina acquista maggiore organicità per rispondere alle esigenze applicative*, *GDir*, 2008, 16, 52; E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, *GDir*, 2008, n. 16, 72; S. ATERNO, *sub* art. 8, in A.A.V.V., *Cybercrime, responsabilità degli enti, prova digitale*, a cura di Corasaniti-Corrias Lucente, Padova, 2009, 194 ss.; per una approfondita analisi giuridica e tecnica, cfr., ATERNO-CAJANI-COSTABILE-MATTIUCCI-MAZZARACO, in *Manuale di Computer Forensics*, cit.

(23) *http://legxv.camera.it/resoconti/dettaglio_resoconto.asp?idSeduta=275&resoconto=stenografio&indice=alfabetico&tit=00180&fase=#sed0275.stenografi co.tit00180*

(24) Si vedano gli ampi stralci della discussione parlamentare rinvenibili sui siti istituzionali della Camera dei Deputati o comunque presenti per esteso in, ATERNO-CAJANI-COSTABILE-MATTIUCCI-MAZZARACO, in *Manuale*, cit.

(25) T. Riesame Roma, 8-7-2008 (dep. 14-7-2008), inedita.

(26) Tale termine, invero, risultava anche dal sito web ufficiale del Consiglio d'Europa a riprova però dell'entrata in vigore della Convenzione e la sua efficacia nei confronti degli Stati membri per quanto riguarda gli obblighi assunti.

(27) Cass. pen., sez. II, 13-3-2009, n. 11135, *GDir*, 2009, n. 17, 84 ss. con un commento di A. CISTERNA, *Tecniche di ricerca appropriate in base all'attuale quadro normativo*.

(28) Si veda in questo senso quella parte dei resoconti stenografici in cui il relatore in aula rileva: «Signor Presidente, la norma in esame è stata oggetto di un'ampia discussione nelle Commissioni perché effettivamente pone delle questioni procedurali estremamente delicate; si tratta di effettuare la perquisizione di sistemi informatici, e, sulla base della disposizione, l'ufficiale di polizia giudiziaria potrebbe accedervi immediatamente. È evidente che sorgono delle preoccupazioni proprio in relazione alla perquisizione, perché la stessa potrebbe alterare i dati, con conseguenze facilmente immaginabili. Noi potremmo anche ipotizzare di aggiungere un inciso alla fine di questa disposizione; vale a dire che la perquisizione debba avvenire con una procedura che assicuri la loro immodificabilità».

3. (Segue). *Sequestro e acquisizione di un sistema informatico e dei dati digitali.*

Grazie alle modifiche introdotte dalla l. n. 48 del 18-3-2008, il codice di procedura penale prevede importanti disposizioni in materia di perquisizione, sequestro, acquisizione e conservazione dei dati presenti su supporti informatici.

In tema di ispezioni, all'art. 244 c.p.p. si è stabilito che l'autorità giudiziaria può disporre le cosiddette ''ispezioni informatiche'' ovvero rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. Relativamente invece alla perquisizione cosiddetta informatica la modifica ha interessato l'art. 247 c.p.p. che al nuovo co. 1 bis stabilisce che ove si ha motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, deve esserne disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

L'intenzione del Legislatore è quella di preservare la cosiddetta ''scena criminis informatica'' sia nei casi sempre più frequenti di rinvenimento di sistemi informatici/telematici o smartphone accesi e collegati alla rete internet, sia nelle diverse ipotesi di rinvenimento di un personal computer spento. È di facile comprensione infatti la differenza che intercorre tra l'ipotesi in cui si rinviene un sistema informatico spento oppure che quest'ultimo si trovi acceso e funzionante o che per le sue qualità e funzioni sia impossibile da sequestrare oppure da spegnere.

È soprattutto in questa ipotesi che può parlarsi più correttamente di perquisizione informatica o di ispezione e di applicazione dell'art. 247 o 244 c.p.p. Di ciò parleremo pertanto nel par. 3. a proposito dell'acquisizione del contenuto di un computer acceso, collegato a piattaforme di cloud computing o comunque non facilmente asportabile.

Durante un'attività di perquisizione domiciliare, in caso di ritrovamento di un personal computer spento, si deve procedere ad un comunissimo sequestro del sistema che, rigorosamente senza mai essere acceso, verrà successivamente sottoposto ad un accertamento tecnico ai sensi dell'art. 359 c.p.p. o ai sensi dell'art. 360 c.p.p sempre osservando quei criteri di garanzia e integrità della digital evidence introdotti nel codice di procedura penale.

Caratteristica tipica del sequestro è la creazione di un vincolo di indisponibilità su una cosa mobile o immobile, che viene ritenuta dagli inquirenti corpo del reato o cosa pertinente al reato, attraverso un atto giudiziario che determina uno spossessamento coattivo del bene stesso. Questo strumento processuale arricchito oggi delle disposizioni sul bisogno di integrità degli elementi di prova digitali, assicura possibili e future prove al procedimento penale garantendo, li dove è possibile, anche la loro conservazione in una forma che consente di mantenere immutate le caratteristiche della cosa e del suo contenuto.

Il sequestro di un sistema informatico risente oggi delle modifiche apportate dalla legge n. 48/2008, ciò che viene posto sotto sequestro probatorio è il documento informatico contenuto all'interno del sistema e non il personal computer o l'hard disk (29). È necessario pertanto assicurare la genuinità sia del supporto e sia del documento esistente all'interno del supporto. In certi contesti investigativi e nel caso in cui sia possibile, la prassi ha consentito più volte la

restituzione del materiale informatico in sequestro (o meglio di una copia di esso) con conseguente conservazione agli atti di una copia clone identica all'originale. La possibilità dell'estrazione di copia degli atti o dei documenti sequestrati e della loro restituzione è stata oggetto di alcune importanti pronunce della giurisprudenza (di merito e di legittimità). La nota sentenza delle Sezioni Unite della Cassazione del 2008 (30) sostiene che la restituzione del materiale informatico (o di parte di esso) in copia, salvaguarda sia l'esigenza d'indagine sia il diritto del soggetto di continuare a disporre comunque degli strumenti lavorativi o dei documenti aziendali e professionali. La richiesta di riesame del sequestro, aggiunge la Corte, è pertanto inammissibile per sopravvenuta carenza di interesse, il quale non è configurabile neanche qualora l'autorità giudiziaria disponga, all'atto della restituzione, l'estrazione di copia degli atti o documenti sequestrati, dal momento che il relativo provvedimento è autonomo rispetto al decreto di sequestro, né è soggetto ad alcuna forma di gravame, stante il principio di tassatività delle impugnazioni.

Prima ancora delle Sezioni Unite del 2008, la Suprema Corte si era pronunciata con un'altra sentenza (31) poco conosciuta con la quale i giudici di legittimità avevano sostenuto che l'acquisizione mediante riproduzione su supporto cartaceo dei dati informatizzati di cui si è presa visione nel corso dell'ispezione di un archivio informatico legittimamente eseguita, non dà luogo a un'ipotesi di sequestro perché non si traduce nell'apprensione dell'archivio stesso (sottraendolo a chi ne è in possesso), ma nella semplice estrazione di copia di dati in esso contenuti, acquisita ai sensi dell'art. 244, 1° co., c.p.p. a seguito di un'operazione tecnica di riproduzione effettuata nello stesso luogo. I giudici della Suprema Corte hanno aggiunto che, in tali casi, non si pone neanche un problema di restituzione dei supporti cartacei realizzati con la stampa dei file in quanto non sono cose sequestrate; e anche qualora si volesse ritenere configurabile un'ipotesi di sequestro dell'archivio informatico, si deve comunque ritenere che esso deve protrarsi solo per il tempo necessario ad estrarre copia dei dati in esso contenuti senza rimozione dal luogo in cui si trova, e che l'acquisizione cessa con l'esaurimento della relativa operazione tecnica di "clonazione" dei dati.

È di tutta e evidenza che in queste situazioni processuali non vi è neanche una vera e propria restituzione di cose sequestrate, dato che dopo l'estrazione delle copie dei dati l'archivio torna immediatamente nella disponibilità dell'avente diritto, spesso nello stesso luogo. Contro tale orientamento della giurisprudenza si è invece schierata la dottrina più attenta (32) ritenendo che sussiste quasi sempre un interesse ad impugnare il trattenimento della copia clone mediante riesame al fine di verificare la pertinenza del dato, oppure a chiedere la restituzione ovvero l'annullamento del provvedimento o comunque chiedere il dissequestro del supporto ove difettino i presupposti previsti dalla legge.

La stessa dottrina sottolinea come la clonazione delle tracce informatiche non sia soltanto una semplice conservazione di tracce bensì più propriamente un vero sequestro di materiale conoscitivo che pertanto deve essere soggetto alle norme di legge sul sequestro e sul riesame a prescindere dalla sua intrinseca capacità di essere facilmente duplicato e restituito.

Di tale avviso è stata anche una parte della giurisprudenza che ha ritenuto esistente l'interesse ad impugnare il sequestro della copia di un hard disk del computer di un giornalista in quanto, anche se le cose oggetto di sequestro erano state restituite previa estrazione di copia dei relativi supporti informatici, vi era l'interesse della richiedente (non indagata nel medesimo procedimento) a fare verificare che l'uso del mezzo tendente all'acquisizione della prova fosse avvenuto nei casi ed entro i limiti previsti dalla legge (33).

La suscettibilità del dato informatico ad alterarsi o modificarsi, anche autonomamente nel momento dell'accensione del computer, impone agli investigatori un'attenzione particolare durante l'acquisizione del suo contenuto.

Un personal computer, un notebook, un telefono mobile (cosiddetto cellulare), uno smartphone, solitamente conservano un'enorme massa di dati utilissimi a risalire ad ogni attività che è stata svolta con quello strumento informatico. Ciò accade anche se l'utilizzatore è stato così accorto da cancellare la memoria dati interna. Se poi questi strumenti sono eternamente connessi alla rete (via wifi o Sim dati) è di tutta evidenza che i dati in essi conservati sono molto più numerosi.

Non esiste uno standard o una metodologia condivisa per il trattamento delle prove digitali forensi, ma esiste solo un insieme di strumenti e procedure più o meno consolidate e testate attraverso l'esperienza e la sperimentazione (34). La prima fase è quella dell'individuazione del reperto informatico d'interesse.

Successivamente, c'è la fase acquisitiva che consiste in un'operazione di estrapolazione e riproduzione su idoneo supporto del dato digitale oggetto di indagine. Ove possibile tutto deve svolgersi nella piena garanzia di integrità e non alterabilità delle tracce e nella prospettiva di una eventuale ripetibilità dell'operazione (magari in sede peritale) e tenendo presente la necessità di garantire la genuinità del dato informatico. Questa fase acquisitiva viene effettuata attraverso software e hardware dedicati che effettuano la cosiddetta bit-stream image (una sorta di "clonazione" del supporto informatico sotto sequestro

dalla quale scaturisce una ''immagine'' del contenuto dell'hard disk su altro supporto preparato all'occorrenza). Tale procedura consente di operare l'analisi forense su un supporto praticamente identico all'originale senza però alterarlo come invece accadrebbe con un'operazione di masterizzazione o di comune salvataggio del file. Una volta eseguita l'acquisizione dei supporti in sequestro è importante recuperare le prove e le informazioni (anche quelle cancellate) attraverso l''' analisi forense'' dei dispositivi digitali acquisiti. È da sottolineare che questa analisi deve essere compiuta con metodi che consentano di conservare, documentare, validare e interpretare gli elementi di prova presenti sulla scena criminis informatica.

In tali situazioni è possibile effettuare l'analisi anche su tutte quelle parti apparentemente ''vuote'' che potrebbero nascondere file o frammenti di file cancellati e quindi assumere una importanza fondamentale ai fini delle indagini e dell'accertamento dei fatti. Eventuali errori compiuti in queste fasi potrebbero produrre effetti negativi in ordine alla prova.

In caso di reperto informatico male acquisito, mal conservato e mal analizzato e considerata la volatilità del dato informatico e la sua modificabilità nel tempo, si potrebbe giungere ad una valutazione di inattendibilità del dato da parte del giudice chiamato a decidere sulla prova.

Infatti se durante l'operazione viene dimostrata la compromissione della genuinità e dell'integrità dei dati contenuti sui supporti informatici sarà possibile mettere in discussione l'utilizzabilità degli elementi probatori raccolti.

L'integrità dell'elemento di prova digitale ha una sua importanza anche in relazione al delicato tema della corretta custodia giudiziaria del reperto e di quelli informatici in particolare. Deve essere dedicata massima cura alla cosiddetta catena di custodia (chain of custody) ovvero alla metodologia di custodia e di trasporto, sia fisico che virtuale delle digital evidences (35).

Un attimo prima dell'inizio delle operazioni tecniche e subito dopo aver acquisito il contenuto forense del reperto viene creata dal software una specie di impronta digitale dell'hard disk che serve a contraddistinguere univocamente la traccia dell'analisi forense appena effettuata e che garantisce per il futuro l'integrità del dato andando a ''certificare'' con una funzione matematica la non alterazione del supporto durante l'acquisizione. Tale operazione si chiama hashing o creazione di un algoritmo di hash.

Il procedimento di hashing si basa su un algoritmo a chiave simmetrica, con algoritmo di classe MD5 e che genera un'impronta della lunghezza di 128 bit. Questa impronta costituisce un riferimento certo alla traccia originale ed è in grado di evidenziare eventuali ricostruzioni o duplicazioni garantendone di fatto l'inalterabilità. Essendo prodotta automaticamente dal software dedicato all'acquisizione del contenuto può essere ritenuta una vera propria certificazione di una procedura attraverso un procedimento matematico che in quanto tale è incontestabile soltanto fino alla dimostrazione del contrario.

Per poter ipotizzare successivamente un'alterazione dei dati ed una generale inattendibilità del contenuto del supporto informatico sarà necessario effettuare un'altra copia forense sull'originale in sequestro e confrontare l'impronta digitale (hash) di quest'ultima acquisizione con l'hash prodotto dalla prima acquisizione. Se queste due funzioni algoritmiche saranno identiche si avrà la prova scientifica che il supporto non è stato alterato; viceversa, se saranno diverse, vorrà dire che, anche accidentalmente, il supporto sotto sequestro è stato modificato.

In Italia sul tema nel 2009 si è avuta una prima pronuncia della Suprema Corte di Cassazione (36) con la quale si è sostenuto che l'esperibilità delle procedure di hashing, è una questione di merito (37), potendosi in sede di legittimità esclusivamente deliberare se gli accorgimenti adottati dalla polizia giudiziaria delegata siano o meno idonei in astratto a tutelare le finalità indicate dal legislatore negli artt. 247, co. 1 bis, e 354, 2º co., c.p.p. per come modificati dalla legge n. 48/2008 di ratifica della Convenzione del Consiglio d'Europa sul cybercrime. Nel paragrafo successivo affronteremo il tema dell'utilità di questa procedura applicata alla forensics dei sistemi informatici in funzione, chiamata anche live forensics.

È importante in questa sede aggiungere alcune considerazioni riguardanti la richiesta di consegna di dati e programmi informatici in alternativa alle ipotesi di sequestro.

La legge n. 48/2008 ha apportato alcune modifiche al codice di rito anche in tema di richieste di consegna di dati e programmi informatici e specificatamente all'art. 248 c.p.p.

Il Legislatore italiano aveva già da tempo stabilito che se l'Autorità Giudiziaria mira ad acquisire una cosa ben precisa e determinata può, nei limiti del possibile e al fine di evitare di compiere atti particolarmente invasivi della sfera delle persone come appunto perquisizioni o ispezioni, invitare il possessore a consegnare ciò che è oggetto di indagine. Lo strumento è molto utile ed efficace anche in presenza di dati informatici ma come si può ben comprendere presenta alcune particolarità.

La legge n. 48/2008 ha novellato la norma inserendo al 2º co., a proposito della documentazione esaminabile presso le banche, «dati, informazioni e programmi informatici». Pertanto, ai sensi del primo comma dell'art. 248 c.p.p., se attraverso la perquisizione si ricerca una cosa determinata, l'autorità giudiziaria

può invitare il possessore a consegnarla. Nel caso in cui la cosa viene presentata, non si procede alla perquisizione salvo che si ritenga utile procedervi per la completezza delle indagini.
Il 2º comma del medesimo articolo prevede che l'autorità giudiziaria o gli ufficiali di polizia giudiziaria da questa delegati possono esaminare presso le banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici. In caso di rifiuto, l'autorità giudiziaria procede ed effettua una perquisizione.
Nella previsione del 1º comma vi è una discrezionalità della Autorità Giudiziaria di richiedere la consegna della cosa ricercata prima di eseguire la perquisizione (dice, «può invitare a consegnarla»). Se la cosa viene consegnata, gli inquirenti hanno davanti due strade entrambe percorribili: la prima è caratterizzata dalla rinuncia alla perquisizione e quindi da una rinuncia alla ricerca di ulteriore materiale, con la seconda strada invece si procede comunque alla perquisizione ritenendola utile per la completezza delle indagini. La norma che qui si commenta è una disposizione che consente di evitare provvedimenti coattivi acquisitivi. Si pensi per esempio alla ricerca di documentazione presso soggetti terzi rispetto al reato o in ipotesi di situazioni soggettive e oggettive delicate.
Infatti, non è detto che la presentazione della cosa ricercata scongiuri del tutto un'attività invasiva successiva. La scelta sull'esecuzione della perquisizione spetta agli inquirenti e viene ovviamente valutata caso per caso.
Il 2º comma invece riguarda esclusivamente la ricerca di documenti (anche informatici) custoditi presso le banche e l'obbligo della preventiva richiesta di consegna da parte della Autorità Giudiziaria. In questi casi la richiesta non è più affidata ad una scelta facoltativa dell'Autorità Giudiziaria; essa infatti può disporre la perquisizione solo in caso di rifiuto dell'istituto bancario a consegnare quanto richiesto. La norma risente quasi sicuramente della preoccupazione del Legislatore per le esigenze di riservatezza e di segretezza che tutelano la raccolta del risparmio e l'esercizio del credito.
È certamente delegabile alla polizia giudiziaria l'esame dei dati delle informazioni e dei programmi informatici nonché degli atti, documenti e della corrispondenza bancaria quando consentito dalla stessa banca.
Viceversa, in caso di rifiuto dell'istituto bancario, si discute sulla delegabilità o meno dell'attività alla polizia giudiziaria. In assenza di sentenze di legittimità sul punto, la dottrina, aderendo ad una interpretazione letterale della norma, ritiene che la successiva perquisizione non è delegabile e che deve procedervi direttamente l'autorità giudiziaria (38).
La locuzione «dati, informazioni e programmi informatici» è completamente assente nel primo comma che parla soltanto di «ricerca di una cosa determinata». Non è chiaro se il Legislatore ha voluto riservare la richiesta di consegna di dati informatici solo nelle ipotesi di istituti bancari e quindi escluderla in tutti gli altri casi, oppure si tratta di una necessità di indicazione specifica dovuta alla riservatezza e alla rigidità del mondo bancario e al regime di acquisizione dei relativi documenti.
Ad avviso di chi scrive quest'ultima interpretazione sembra la più corretta e la più logica. È infatti abbastanza pacifico che un'interpretazione estensiva del 1º comma dell'art. 248 c.p.p. consente comunque di far rientrare tra le ''cose determinate'' anche i dati informatici non sussistendo ragioni per escluderli da tale categoria generale.

(29) P. Tonini, *Manuale di Procedura penale*, Milano, 2011, 367.
(30) Si veda tra tutte, Cass. pen., S.U., 7-5-2008, n. 18253, *DPP*, 2009, 4, 469, fattispecie relativa a sequestro di un computer e di alcuni documenti con restituzione della cosa sequestrata.
(31) Cass. pen., sez. III, 19-6-2000, n. 384, *CED*, 217687.
(32) P. Tonini, *op. ult. cit.*, 367; nello stesso senso, si veda S. Carnevale, *Copia e restituzione dei documenti informatici sequestrati: il problema dell'interesse ad impugnare*, *DPP*, 2009, 472.
(33) Cass. pen., sez. VI, 31-10-2007, n. 40380, *CED*, 237917, secondo la quale «Il sequestro probatorio disposto nei confronti di un giornalista professionista deve rispettare con particolare rigore il criterio di proporzionalità tra il contenuto del provvedimento ablativo di cui egli è destinatario e le esigenze di accertamento dei fatti oggetto delle indagini, evitando quanto più è possibile indiscriminati interventi invasivi nella sua sfera professionale. (Fattispecie in cui è stato ritenuto illegittimo il sequestro del computer in uso ad una giornalista e dell'area del ''server'' dalla stessa gestita, con la conseguente acquisizione dell'intero contenuto dell'''hard disk'' e di un'intera cartella personale presente nell'area del sistema operativo)».
(34) In questo senso si veda anche una prima pronuncia della cassazione, Cass. pen., 12-12-2008, n. 11135.
(35) Si veda, Cass. pen., 16-12-2009, n. 2388, in un caso di perizia e di materiale informatico (dvd e cd) conservato male e non sigillato correttamente.
(36) Si veda, Cass. pen., 12-12-2008, n. 11135.
(37) Era stata posta all'attenzione della corte la mancata adozione di una procedura di garanzia finalizzata a verificare l'integrità e la conformità all'originale del dato informatico acquisito da un PC aziendale non sequestrato ma riprodotto in copia su un Cd-Rom.
(38) Conso-Grevi (a cura di), *Commentario breve al Codice di procedura penale. Complemento giurisprudenziale*, Padova, 2009, 744.

4. (Segue). *Ispezione, perquisizione e acquisizione di un sistema informatico e telematico in funzione non sequestrabile: banche dati complesse, servers e piattaforme di cloud computing.*
Le ipotesi in cui è possibile rinvenire sistemi informatici o telematici accesi e funzionanti sono sostanzialmente di due tipi: la prima è il caso ormai di scuola frequente relativo a comunissimi personal

computers o apparati informatici che si rinvengono accesi sulla scena del crimine ma che sostanzialmente sono facilmente asportabili e quindi nella maggioranza dei casi oggetto di sequestro e di successiva acquisizione e analisi forense; la seconda ipotesi è quella molto frequente in cui le circostanze di fatto e di luogo non consentano di acquisire il contenuto di un sistema informatico attraverso la consegna materiale dei dati o comunque non consentono di sequestrare dati e supporti informatici (server) senza provocare un blocco del servizio (spesso) pubblico o di pubblico interesse (si pensi all'ipotesi di operatori di telefonia, internet service provider, società che allocano spazio in sistemi di cloud computing, gestori di comunicazioni accessibili al pubblico).

Le norme del codice di procedura penale e i cosiddetti standard operativi certificati disciplinano la ''cristallizzazione della digital evidence'' e mirano a garantire l'integrità dei dati.

Si procede attraverso l'osservanza di tecniche di spegnimento del sistema in grado di preservare la memoria Ram, fino a soluzioni tecnologicamente avanzate per i casi più complessi e delicati.

In caso di intervento in questi ambiti è frequente che non si conosca esattamente in quale server sono memorizzati i files d'interesse e vi sia l'impossibilità concreta di sequestrare (o anche solo ispezionare) tutto il contenuto del server o dei diversi servers in uso.

Si pensi in primo luogo alle difficoltà di sequestrare una ingente mole di dati informatici presso provider (hosting o content provider) che gestiscono siti internet, posta elettronica e tanti altri servizi, oppure presso gestori di comunicazioni accessibili al pubblico. Si pensi anche ai tanti server o alla banca dati di un istituto finanziario, di una grande azienda (magari internazionale con server in parte all'estero), di un internet service provider o di una enorme mole di dati presente su cloud computing e quindi per sua natura allocata su server indeterminato e indeterminabile. Nella maggior parte dei casi non è neanche pensabile interrompere il servizio soprattutto nei casi in cui si ricerca la prova presso terzi e non direttamente nei sistemi di proprietà dell'indagato.

In tali situazioni affinché l'indagine non si blocchi di fronte a difficoltà di ordine pratico è necessario che l'organo procedente si ponga preventivamente di fronte all'interrogativo su *cosa* sequestrare.

È di tutta evidenza che soprattutto in tali situazioni e di fronte a tali numeri non tutto costituisce corpo del reato e non tutto è opportuno sequestrare o acquisire. Deve effettuarsi una scelta preventiva dei dati che possono essere utili alle indagini e ciò che invece può essere trascurato (39).

Dunque è necessario comprendere con esattezza cosa cercare e con quali modalità acquisire ciò che si desidera al fine di consentire però la ripetibilità dell'operazione e garantire la genuinità degli elementi di prova. Cosa cercare è chiaramente un problema investigativo che varia da caso a caso ma che non rileva soltanto sotto il profilo della ricerca del corpo del reato, ma anche di tutte quelle tracce utili alle indagini che vengono lasciate dallo strumento informatico e che un bravo investigatore (sia esso dell'accusa o della difesa) deve saper cercare e individuare. Relativamente alle modalità di acquisizione, esse variano a seconda se ci troviamo di fronte ad un atto ripetibile o ad un atto irripetibile.

Una volta individuati i file o le directory da acquisire in quanto utili e necessarie alle indagini occorre farlo garantendo l'integrità del file e la non modificabilità. Escludendo l'ipotesi di poter salvare il file su un supporto esterno (es. pen drive) con il tipico comando ''salva con nome'' in quanto andrebbe a modificare i cosiddetti metadati alterando il file e il suo contenuto, è possibile invece effettuare una tipica masterizzazione del files o dell'intera cartella?

La giurisprudenza della Corte di Cassazione si è pronunciata sul punto e in un caso di documenti informatici utili alle indagini rinvenuti all'interno di un personal computer acceso durante una perquisizione ha stabilito che la masterizzazione del file non costituisce attività irripetibile bensì attività ripetibile e che pertanto è formalmente corretta (40). Con un'altra recente pronuncia la Suprema Corte si è confrontata con l'acquisizione di un file di posta elettronica su un server aziendale di una grande banca italiana in un procedimento che riguardava il furto d'identità, il trattamento illecito di dati personali e alcune presunte truffe ai danni di utenti e-bay. Il caso affrontato dai giudici di legittimità riguardava una richiesta di sequestro del pubblico ministero erroneamente fondata sull'art. 254 bis c.p.p. (sequestro presso fornitori di servizi informatici, telematici e di telecomunicazioni) in quanto in realtà rivolta ad un istituto bancario che presso i propri server conservava il file delle email in formato ''.pst'' delle cartelle outlook di posta elettronica dell'indagato. Il caso è stato oggetto di due pronunce giurisprudenziali: la prima è stata una sentenza del Tribunale del Riesame di Roma (41) del 2008 poi impugnata ed a cui è seguita una pronuncia della Suprema Corte di Cassazione (42).

Nelle motivazioni di quest'ultime due sentenze della Cassazione ci sono alcuni aspetti che riguardano l'acquisizione di alcuni files o documenti informatici che dovevano essere chiariti e spiegati meglio.

Per esempio, con riferimento alla seconda sentenza citata, quella del file di posta elettronica nel server della banca, i giudici di legittimità hanno ritenuto che ogni valutazione di ordine tecnico circa la necessità di effettuare l'hashing per poter eventualmente verificare se la copia del file nel compact disk masterizzato sia uguale all'originale (e quindi se il file sia

stato modificato o meno) è estranea al giudizio di legittimità, sia perché attiene essenzialmente alle modalità esecutive del sequestro sia perché comunque la normativa richiamata dal ricorrente non individua specificatamente le misure tecniche da adottare, limitandosi a richiamare le esigenze da salvaguardare attraverso idonei accorgimenti; la Corte ha aggiunto comunque che nel caso di specie, la sezione della polizia postale (di Isernia) nell'acquisizione della documentazione informatica relativa all'attività delittuosa oggetto di indagine aveva in concreto adottato le cautele previste dalla legge n. 48/2008.

In realtà la Suprema Corte in entrambe le sentenze sopra richiamate, non ha tenuto conto che la procedura posta in essere non era affatto idonea a tutelare le finalità indicate dal legislatore negli artt. 247, co. 1 bis, e 354, 2º co., c.p.p. proprio in considerazione della mancata adozione di ciò che stabiliscono questi due ultimi commi citati. Al di là del rilievo fatto dagli ermellini che la questione attiene al merito e quindi al giudice del dibattimento sarebbe stato opportuno chiarire meglio ciò che il quest'ultimo giudice deve verificare in concreto in sede di giudizio anche perché non vi è dubbio che già da una lettura delle carte processuali non emergeva alcuna modalità di conservazione del file originale.

Se non si adottano le misure tecniche o non si impartiscono le prescrizioni necessarie ad assicurare la conservazione e ad impedire l'alterazione e l'accesso a dati, informazioni e programmi informatici viene violato proprio il dettato normativo ed in particolare un accorgimento di garanzia finalizzato a verificare l'integrità e la conformità all'originale del dato informatico (file che contiene tutta la posta elettronica di un dipendente) acquisito da un server aziendale (non sequestrato).

La riproduzione in copia su un Cd-Rom firmato da tutti operanti di polizia giudiziaria e dall'ausiliario di p.g. potrebbe non essere sufficiente a garantire il principio di garanzia ma soprattutto non ha senso se non viene adottato quanto affermato nella seconda parte dell'art. 247, co. 1 bis, e nella prima parte del 2º co. dell'art. 354 c.p.p. [«(...) adottare altresì le misure tecniche o impartire le prescrizioni necessarie ad assicurare la conservazione e ad impedire l'alterazione e l'accesso (...)»].

È di tutta evidenza che non si è tenuto in debito conto che il file di tutta la posta elettronica (es. outlook) presente sul sever, ''l'originale'', per sua propria natura e fin tanto che viene lasciato al suo posto e non viene definitivamente tolto da quella sede è soggetto a continue modifiche anche del tutto involontarie e indipendenti dall'azione dal titolare della casella di posta o di soggetti terzi.

Pertanto, senza un ''congelamento'' e un'asportazione del file con un preliminare calcolo di hash (43), non si consente alla difesa di ripetere l'operazione direttamente dal server di posta elettronica ma soltanto dalla copia del cd-rom effettuato tempo prima dalla polizia giudiziaria e di non verificare il file originariamente acquisito attraverso la ripetizione della procedura e il confronto degli hash.

Tutta la fase che precede un'acquisizione informatica su computer acceso (cosiddette live forensics) dovrebbe essere debitamente documentata. Ove non si voglia ricorrere al video effettuato dalla polizia giudiziaria con una telecamera tipicamente durante i rilievi e gli accertamenti della polizia scientifica, esistono software che consentono di documentare e dimostrare ciò che accade sullo schermo di un personal computer registrando un video immediatamente disponibile poi su supporto informatico; procedura e video che potrebbe essere poi certificato applicando una firma digitale. Esistono anche i cosiddetti keylogger (software o hardware) in grado di registrare tutto ciò che un utente digita sulla tastiera del computer e quindi essere utilizzati all'occorrenza anche per certificare l'autenticità e la genuinità di un'operazione di acquisizione fatta dalla polizia giudiziaria durante una live forensics. In considerazione dell'alta probabilità di errore nelle acquisizioni informatiche cosiddette live, questa tecnica anche qui andrebbe suggellata con l'apposizione della firma digitale ai file di log prodotti dal software al fine di certificare l'operato della polizia giudiziaria al di là di quanto potrebbe fare un semplice verbale di polizia dal quale certamente non emergerebbero gli errori inconsapevoli eventualmente commessi.

La legge di ratifica della Convenzione di Budapest ha introdotto il concetto di ispezioni informatiche accanto a quello di perquisizioni informatiche (art. 244 2º co. c.p.p. e art. 247 c.p.p.).

Alcune brevi riflessioni inducono a ritenere che in realtà una pur minima differenza tra i due strumenti di ricerca della prova può esserci.

L'ispezione consiste nel limitare l'operante all'esame obiettivo della situazione di fatto esattamente come essa ricade sotto i sensi percettivi dell'operante che sta procedendo. L'atto ispettivo viene disposto ed effettuato a scopo di percezione visiva personale e di tutto ciò che può essere rilevante per le indagini (art. 244 c.p.p.) con possibilità di eseguire rilievi segnaletici, descrittivi e fotografici ed etimologicamente deriva da ''in-spicio'' ovvero qualcuno guarda ''in'' qualcosa. Mentre, nella perquisizione, il perquirente ''fruga'' e l'osservazione visiva è il semplice mezzo per l'attività di ricerca e di apprensione materiale.

L'attività ispettiva è per lo più un rilevamento morfologico degli effetti e delle tracce esterne visibili, senza intervento modificatore o invasivo dell'investigatore.

Alcune leggi speciali prevedono che la polizia giudi-

ziaria può procedere a ''controlli'' e ''ispezioni'' (denominate anche ''di sommaria ricerca'') che possono ''progredire'' in vere e proprie perquisizioni quando ciò è necessario in conseguenza di risultati derivanti dall'originario intervento investigativo. In questi casi le ispezioni devono considerarsi atti atipici di indagine e si sostanziano in un'attività di osservazione e percezione che può essere eseguita sia da agenti sia da ufficiali di p.g. e che in via generale può riguardare esclusivamente i mezzi di trasporto, i bagagli e gli effetti personali (44).

Le ispezioni personali consistono nell'accertamento, sulla sfera intima del corpo di una persona, delle tracce o degli effetti che il reato ha lasciato. Sono diversi e preclusi alla polizia giudiziaria gli accertamenti medici invasivi.

Sulle persone gli organi investigativi possono compiere consensualmente o anche coattivamente i cosiddetti rilievi esteriori ovvero quelle attività di osservazione e descrizione che non comportano restrizioni fisico-morali alla libertà del soggetto o che non si attuano con metodi invasivi. Ad esempio, rientrano in tale ultimo tipo di ispezione la descrizione di una persona o di parte del suo corpo o l'accertamento della presenza di macchie o cicatrici. Mentre tra i rilievi esteriori non rientrano, ad esempio quelli che debbono essere compiuti su parti interne del corpo o su parti nascoste. Sono invece consentiti gli accertamenti medici non invasivi quali ad esempio le ispezioni radiografiche (anche se solitamente si procede previa delega del pubblico ministero) (45).

L'ispezione tende quindi ad assumere informazioni utili attraverso la lettura di segni che abbiano significati ricavabili dall'applicazione di criteri argomentativi: se in un luogo si rinviene della cenere o del fumo ciò fa pensare che vi è stato del fuoco.

Ciò detto, possiamo ipotizzare un'attività ispettiva su di un sistema informatico? Quando, in che forme e modalità? (46).

Si pensi al caso in cui gli organi inquirenti rilevino un segno sul personal computer o la presenza di un hardware o strumento particolare e che in ragione delle loro conoscenze informatiche da ciò solo sia possibile argomentare che su quel computer è stata eseguita una determinata operazione con una determinata finalità proprio perché è possibile, sulla base di cognizioni tecniche specifiche, attribuire a quella traccia un significato che va al di là di ciò che appare.

Poniamo il caso che il sistema sia acceso ed in funzione e la polizia giudiziaria d'iniziativa sia interessata a conoscere quante più informazioni possibili prima di richiedere eventualmente un decreto di perquisizione al magistrato.

Un'attività invasiva di accesso interno al sistema e di utilizzo degli strumenti informatici potrebbe provocare un'alterazione del sistema stesso o dei dati ed una modifica dei file o del loro contenuto (soprattutto se il file o la ''cartella'' vengono aperti). In questo caso, il sistema, se stimolato da una operazione anche semplice come il clik del mouse, autonomamente effettua tutta una serie di operazioni in grado di modificare informazioni interne al sistema stesso. Ciò potrebbe porre in essere un'attività contrastante con il nuovo disposto dell'art. 244 c.p.p. che stabilisce la necessità di adottare *misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*.

L'attività posta in essere in questo caso sembra andare oltre il semplice ''sguardo esplorante'' tipico dell'ispezione. L'attività che si pone in essere in questi ambiti informatici e telematici sembra andare oltre il semplice scrutamento del contenuto, delle forme, delle qualità e caratteristiche del mezzo per arrivare invece ad un'attività più vicina a quella tipica di perquisizione.

La previsione nell'art. 244 c.p.p. di tale tecnica di preservation data, potrebbe far ritenere che con l'ispezione si possa scrutare, guardare all'interno di un sistema informatico pur impedendo l'alterazione del dato. Ciò, potrebbe indurre a ritenere sussistente una sovrapposizione con l'istituto della perquisizione informatica anch'essa oggetto di riforma con le modifiche degli artt. 247, co. 1 bis, 248, 2º co., e 352, co. 1 bis (47).

Ad avviso di chi scrive, l'attività di ricerca di un qualcosa di preciso e circostanziato all'interno di un sistema informatico o di un server sembra essere riferibile più all'ipotesi di perquisizione piuttosto che di ''inspectio'', mentre una ricerca più generica e superficiale è più vicina all''ispezione informatica disciplinata dall'art. 244 c.p.p.

In una scena criminis informatica, l'ispezione è possibile limitatamente al rilevamento esteriore di tracce e di altri effetti del reato ed è quindi ipotizzabile soprattutto nel momento in cui ci si limita ad osservare il sistema informatico o telematico o comunque ciò che accade nel suo monitor, descrivendolo nei suoi particolari, ad esempio la presenza di periferiche collegate o scollegate, rilevando la presenza (sistema acceso) di particolari sistemi hardware o software, l'utilizzo e la presenza di sistemi di connessione (reti wireless, adsl) di supporti informatici di pertinenza ed eventualmente tutto ciò che appare in quel momento sul video.

Può ad esempio accadere che prima di procedere al sequestro dell'hard disk, la polizia giudiziaria, sempre avvalendosi di strumenti tecnologici adeguati, effettui una attività di ''preview'', ovvero di ''visione preliminare'' del contenuto del supporto e poi, solo dopo decida di procedere al sequestro in considerazione dell'esito dell'attività ispettiva.

Questa forma di osservazione ''in preview'' (48) è

sostanzialmente un'attività tecnica certamente ripetibile e tipica di colui che "fruga" e che quindi perquisisce ma senza alterare il contenuto del supporto: vi sono tutti i presupposti per definirla una vera e propria perquisizione informatica ma ripetibile in quanto in dibattimento, sul supporto in sequestro (e ben conservato), potrà essere ripetuta "n" volte anche da tutte le altre parti processuali.

(39) Tale scelta può essere effettuata attraverso il ricorso all'ispezione informatica prevista ai sensi dell'art. 244 c.p.p. di cui si dirà più avanti.
(40) Cass. pen., sez. I, 25-2-2009, n. 11503, *CED*, 243495; si veda anche Cass. pen., 12-12-2008, n. 11135.
(41) T. Riesame Roma, 8-7-2008, inedita ma di cui ampi passaggi possono apprezzarsi in ATERNO-CAJANI-COSTABILE-MATTIUCCI-MAZZARACO, in *Manuale*, 2012, cit., 488 ss.
(42) Cfr. Cass. pen., sez. II, 13-3-2009, n. 11135, *GDir*, 2009, n. 17, 87 e in *www.giuristitelematici. it/modules/bdnews/article.php?-storyid=1648*: trattasi della prima sentenza della Suprema Corte dove si fa riferimento a questa tecnica di hashing e si nota con favore che negli ultimi tempi, complici alcuni ricorsi in materia di reati informatici, la Corte di Cassazione è stata chiamata a misurarsi con le nuove tecnologie e con il principio relativo di ripetibilità dell'accertamento. Per un commento su tale sentenza cfr. A. CISTERNA, *Tecniche di ricerca appropriate in base all'attuale quadro normativo*, cit., 87 ss.
(43) Si pensi all'ipotesi di "comprimere" il file, proteggerlo con password lasciandolo così immodificabile nel server.
(44) Si veda, D'AMBROSIO-P.L. VIGNA, *La pratica di Polizia Giudiziaria*, Padova, 2003, 73.
(45) In materia di ispezioni radiografiche si veda per tutte, Cass. pen., sez. VI, 11-7-2005, n. 33988, *CED*, 232234, con la quale la Suprema Corte ha affermato che in materia di stupefacenti, mentre l'ispezione e la perquisizione previste dal codice di procedura penale presuppongono sempre la commissione di un reato, i poteri concessi alla polizia giudiziaria dall'art. 103 del d.p.r. 9-10-1990 n. 309, hanno un ambito più ampio, essendo finalizzati anche ad attività di carattere preventivo ed essendo del resto subordinati solo alla sussistenza del «fondato motivo di ritenere che possano essere rinvenute sostanze stupefacenti o psicotrope».In questa prospettiva, deve ritenersi legittimo che la polizia giudiziaria, dopo l'esito negativo di una perquisizione personale, sussistendo il fondato motivo che il soggetto detenga all'interno del proprio corpo ovuli contenenti sostanza stupefacente, lo sottoponga, previa autorizzazione del P.M., ad esame radiologico, trattandosi di attività diretta non soltanto all'accertamento del reato (nella specie, verificatosi per l'avvenuto rinvenimento degli ovuli, poi fatti espellere in ospedale, sotto il controllo del medico, mediante la somministrazione di lassativi), ma anche alla tutela del diritto alla salute del soggetto.
(46) Si veda, Cass. pen., sez. III, 26-1-2000, n. 384, *CED*, 217687, una delle primissime sentenze della Suprema Corte di Cassazione in materia di ispezioni su dati informatici (seppur sui generis). In tema di mezzi di ricerca della prova, non costituisce sequestro probatorio l'acquisizione, mediante riproduzione su supporto cartaceo, dei dati informatizzati contenuti in un archivio informatico visionato nel corso di una ispezione legittimamente eseguita ai sensi dell'art. 244 c.p.p. Nel caso di specie la Corte ha ritenuto che non si versasse in un'ipotesi di sequestro in quanto non vi era stata alcuna apprensione dell'archivio informatico il quale non era stato sottratto al possessore, bensì di una semplice estrazione di copia dei dati in esso contenuti, sicché non si poneva nemmeno un problema di restituzione dei supporti cartacei realizzati.
(47) La perquisizione informatica prevista dal codice di procedura penale non deve confondersi con la c.d. perquisizione occulta da remoto e della quale ci occuperemo nel par 12.
(48) Per effettuare tale operazione tecnica a computer spento vi sono diversi programmi; i più utilizzati sono, il programma "Encase" della Guidance Software Inc. e il programma FTK (Forensics Tool Kit). È una prassi consolidata soprattutto in procedimenti in materia di pedopornografia. Questi software sono ormai da diversi anni in dotazione alle forze di polizia italiane e la preview viene solitamente effettuata sul posto proprio al momento del rinvenimento di un sistema al fine di valutare preliminarmente la situazione "informatica" che ci si trova di fronte.

5. (Segue). *L'accertamento tecnico urgente sui supporti informatici.*

In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici ritenuti interessanti, gli ufficiali della polizia giudiziaria adottano le misure tecniche o impartiscono le prescrizioni necessarie ad assicurare la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.

Considerata la grande diffusione di strumenti tecnologici di vario tipo l'accertamento urgente di cui all'art. 354, 2º co., assume oggi un ruolo ancora più importante e centrale. In qualsiasi tipo di indagini, nel momento in cui la polizia giudiziaria giunge per prima sulla scena criminis rinviene in moltissimi casi una notevole quantità di supporti informatici e di materiale informatico con memorie o banche dati digitali che potrebbero essere utili per le indagini. Quest'ultime spesso vengono rinvenute accese (si veda ad esempio telefoni cellulari, iphone, ipad, ipod). La giurisprudenza, anche se non pacificamente, ha sempre distinto l'accertamento dai rilievi.

Con il termine accertamento ha per lo più ritenuto lo studio e la relativa elaborazione critica di dati materiali pertinenti ai reati e quindi analisi soggettive e risultanze assunte su basi tecnico scientifiche (49), mentre con il termine rilievi ha definito tutte quelle attività che si esauriscono in una costatazione, raccolta e in semplici operazioni di carattere materiale (50).

Le operazioni urgenti che possono compiere gli organi di polizia di fronte ad un elemento di prova digitale suscettibile di alterazione e modificazione, devono essere comunque attività materiali e tecniche di conservazione del dato nella sua integrità e, ove l'urgenza lo renda necessario (e ciò sia possibile) la duplicazione su un supporto idoneo in maniera tale da rendere l'operazione di duplicazione ripetibile salvaguardando quindi l'integrità del dato sul supporto originale e il diritto della difesa a ripetere l'operazione verificando la genuinità del dato (es. smartphone, telefoni mobili, computers, server, server farm, main-

frame, grandi o piccole banche dati, piattaforme di cloud computing) (51).
Sulle modalità e sulle garanzie delle acquisizioni di dati urgenti su sistemi informatici ex art. 354, 2º co., c.p.p. si richiama quanto detto in precedenza nel par. 3. a proposito dell'algoritmo di hash e della ripetibilità dell'operazione ovvero dell'importanza di creare quell'impronta digitale del file e lasciare più dati possibili affinché la difesa possa verificare la correttezza delle operazioni compiute e l'integrità del dato.
In tema di accertamento urgente ex art. 354, 2º co., c.p.p, gli atti non diventano irripetibili neanche quando le forze di polizia, grazie all'utilizzo di strumenti informatici tecnici di ''preview'' (che attraverso un software non alterano dati e supporti originali), prendono diretta cognizione di situazioni, informazioni e dati all'interno delle memorie informatiche. Durante tale operazione di ''preview'' effettuata correttamente e senza errori tecnici il supporto informatico in esame non viene modificato o alterato. Ciò è comunque facilmente dimostrabile attraverso la ripetibilità dell'operazione e il confronto con gli algoritmi di hash calcolati dai software prima dell'inizio e dopo la chiusura delle operazioni.
La medesima considerazione può essere fatta quando durante una perquisizione il computer viene rinvenuto acceso e sussista la necessità di lasciarlo acceso in quanto il suo spegnimento potrebbe provocare la perdita di dati interessanti, oppure in tutti quei casi di acquisizione di dati presso i provider, o presso istituti finanziari o grandi banche dati con enormi quantità di server difficilmente sequestrabili.
Altra ipotesi di accertamento o rilievo tecnico urgente da porre in essere con le modalità sopra specificate è quella relativa alle perquisizioni presso terzi soprattutto quando la clonazione dell'intero hard disk o dei server è sovrabbondante e c'è il rischio concreto di acquisire dati e informazioni non necessari per l'indagine o addirittura lesivi della dignità o del diritto di riservatezza delle persone. La cassazione si è pronunciata in tali casi a proposito dell'acquisizione di sistemi informatici di professionisti o di giornalisti (52) ed ha stigmatizzato le prospettazioni del pubblico ministero rese in udienza in quanto sollevavano incertezze sull'effettivo contenuto della notitia criminis e sulla presenza della necessità del provvedimento di sequestro a fini probatori anche in considerazione del fatto che l'acquisizione di numeroso materiale informatico (floppy disk, cd-rom, ecc.) e la clonazione dell'intero hard disk del giornalista, implicava pesanti intrusioni nella sfera personalissima del giornalista stesso che al momento non risultava neanche indagato.
L'adozione delle misure tecniche e delle procedure come richiamate dall'art. 354, 2º co., c.p.p. assume proprio in tali ipotesi un'importanza fondamentale in quanto alla luce di quanto sopra descritto, anche nei casi di urgenza, è ben possibile salvaguardare la riservatezza di dati non utili alle indagini ma al contempo acquisire correttamente e con modalità forensi i soli dati digitali d'interesse.

(49) Cass. pen., 9-2-1990, n. 301, *CED*, 183648.
(50) Cass. pen., 10-11-1992, n. 4523, *CED*, 192570.
(51) Cass. pen., sez. I, 5-3-2009, n. 14511, *CED*, 243150; Cass. pen., 25-2-2009, n. 11503, *CED*, 243495.
(52) Si veda in questo senso, Cass. pen., 16-2-2007, n. 25755, *CED*, 237430, e si veda anche, Cass. pen., sez. VI, 11-12-1998, n. 2882, *CED*, 212678; nonché, Cass. pen., 31-10-2007, n. 40380, *CED*, 237917, secondo la quale il sequestro probatorio disposto nei confronti di un giornalista professionista deve rispettare con particolare rigore il criterio di proporzionalità tra il contenuto del provvedimento ablativo di cui egli è destinatario e le esigenze di accertamento dei fatti oggetto delle indagini, evitando quanto più è possibile indiscriminati interventi invasivi nella sua sfera professionale. (Fattispecie in cui è stato ritenuto illegittimo il sequestro del computer in uso ad una giornalista e dell'area del ''server'' dalla stessa gestita, con la conseguente acquisizione dell'intero contenuto dell'''hard disk'' e di un'intera cartella personale presente nell'area del sistema operativo).

6. (Segue). *La custodia delle cose sequestrate ex art. 259 c.p.p.*
La custodia dei beni sottoposti a sequestro è necessaria per assicurare la conservazione e per garantire la funzione probatoria. In caso di sequestro di supporti informatici il problema della loro custodia è delicato tanto che la legge n. 48/2008 è intervenuta anche su questa norma inserendo nel testo del secondo comma dell'art. 259 c.p.p. la seguente disposizione: «quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva in quest'ultimo caso, diversa disposizione dell'Autorità Giudiziaria». La metodologia alla base di questo principio, secondo gli standard di computer forensics, prende il nome di catena di custodia (chain of custody).
È necessario preservare il supporto informatico dall'elevato rischio di alterazioni spesso dovuti a errori di distrazione o ad imponderabili fenomenologie tecniche.
Le garanzie alla base di una corretta ''catena di custodia'' sono a tutela anche degli stessi soggetti nominati come custodi in quanto li pongono al riparo da eventuali responsabilità penali, civili e disciplinari.
Le misure indicate, se adottate con cura, sono inoltre utili a garantire la genuinità e la certezza dell'identità della cosa sequestrata al fine di evitare, come accaduto e descritto da una recente sentenza della Suprema Corte di Cassazione (53), che il perito nominato dal Tribunale rilevi che il materiale informatico consegnatogli era difforme quantitativamente da quanto verbalizzato dalla polizia giudiziaria al momento del

sequestro dei supporti (CD e DVD) contenenti file pedopornografici.
In un diverso ambito, ovvero in materia di estrazione di copia di un hard disk ed esame dello stesso si rinviene una pronuncia utile a comprendere l'importanza del ruolo del custode anche come soggetto che deve impedire l'accesso da parte di soggetti terzi non autorizzati o non tecnicamente qualificati. In questo caso il custode aveva imprudentemente consentito l'accesso al reperto informatico ad una delle parti e la Cassazione ha sostenuto che l'esame dell'"hard disk" di un computer in sequestro e la conseguente estrazione di copia dei dati ivi contenuti non sono attività che le parti possono compiere alla sola presenza del custode, in quanto implicano accertamenti ed interventi di persone qualificate con l'utilizzo di appositi strumenti, e che pertanto devono essere necessariamente svolti in dibattimento, nel contraddittorio, e sotto la direzione del giudice (54).
La norma riguarda un po' tutti gli ambiti che potenzialmente potrebbero essere oggetto di provvedimenti di sequestro o di acquisizione di dati informatici.
Con una certa frequenza la norma si pone a carico di fornitori di servizi di comunicazione (internet service provider, access provider e content provider) destinatari (in quanto intermediari e non come soggetti responsabili) dei numerosi provvedimenti dell'Autorità Giudiziaria che indaga sui reati commessi mediante sistemi informatici.
Dopo aver nominato un soggetto custode deve seguire l'avvertimento circa gli obblighi di impedire l'alterazione dei file o l'accesso da parte di terzi. Tali misure possono essere disposte secondo vari livelli di sicurezza e non ci sono indicazioni standard perché spesso l'esecuzione è lasciata alla piena discrezionalità del custode (55).
Un'altra norma che richiama e disciplina la delicata questione della conservazione delle digital evidence è l'art. 260 c.p.p. relativo all'apposizione dei sigilli alle copie cosiddette digitali mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.
La funzione dei sigilli serve a garantire la genuinità del sequestro, infatti l'apposizione dei sigilli o di altro segno idoneo ha la funzione di manifestare immediatamente il vincolo di indisponibilità sulla cosa oggetto di sequestro e di garanzia della sua continuità nel tempo.
Le novità inserite nell'articolo dalla legge n. 48/2008 sono due. La prima è un nuovo mezzo idoneo ad indicare il vincolo imposto a fini di giustizia ovvero un mezzo di tipo elettronico o informatico.
Per esempio sui dati e sulle informazioni contenute in un server difficilmente sequestrabile, il compito di sigillo e di garanzia può essere assolto da sistemi software come la firma digitale o la crittografia da apporre direttamente sul contenuto informatico dell'intero supporto, sulle cartelle ivi contenute o sul singolo file (sempre facendo attenzione a non alterare o modificare i dati sotto sequestro). Certamente il metodo del sigillo elettronico si addice maggiormente ai casi di sequestri o acquisizioni di materiale online o di supporti riscrivibili (pen drive, digital card, CD WR, ecc., ecc.).
La seconda novità è invece relativa alla procedura di estrazione di copia dei documenti informatici o di programmi. In tali casi le copie devono essere realizzate su adeguati supporti assicurando la conformità della copia all'originale e la sua immodificabilità.
L'intervento dell'Autorità Giudiziaria nel procedimento di verificazione dei sigilli non è necessario, salvo il caso in cui il pubblico ministero o il giudice debbano compiere uno specifico atto che ne comporti la rimozione.
A questo proposito, la Corte di Cassazione ha ritenuto che la polizia giudiziaria può procedere legittimamente a verificare l'integrità dei sigilli precedentemente apposti dalla stessa sui reperti nel momento in cui gli stessi devono essere sottoposti ad accertamenti tecnici ad opera di un altro organo di polizia (56).

(53) Cass. pen., sez. III, 19-1-2010, n. 2388, non massimata.
(54) Cass. pen., sez. III, 13-7-2009, n. 28524, *CED*, 244594.
(55) Cass. pen., sez. III, 28-1-2003, n. 4023, *CED*, 224324; Cass. pen., sez. IV, 27-7-2005, n. 27915, *CED*, 231811.
(56) Cass. pen., sez. I, 15-7-2010, n. 27579, *CED*, 247676.

7. (Segue). *Il sequestro di corrispondenza inoltrata per via telematica ex art. 254 c.p.p.*
Con la legge di ratifica della Convenzione di Budapest sono state aggiunte alcune disposizioni in tema di sequestro di corrispondenza informatica ed elettronica. L'art. 254 c.p.p. ha visto ampliarsi il novero dei soggetti destinatari del provvedimento di sequestro specifico, la tipologia della corrispondenza oggetto di acquisizione (la corrispondenza telematica) e l'inserimento dell'importante principio della "non alterabilità" del reperto. L'articolo prevede che è possibile procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni in tutti i casi in cui l'autorità giudiziaria abbia fondato motivo di ritenere siano spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato.
Quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza

aprirli o alterarli e senza prendere altrimenti conoscenza del loro contenuto.
Il legislatore ha posto una disciplina differenziata per regolamentare il sequestro della corrispondenza in presenza di un bene meritevole di particolare tutela. Non vi è dubbio che la tutela apprestata alla libertà e segretezza della corrispondenza trova il suo fondamento nell'art. 15 Cost. e anche in presenza di ogni tipologia di corrispondenza o comunicazione informatica e in presenza di corrispondenza in transito presso il gestore del servizio di recapito.
Il 1º comma dell'art. 254 c.p.p. è stato modificato dall'art. 8, 4º co., l. 18-3-2008, n. 48 nella parte in cui è stata estesa la categoria dei soggetti presso i quali effettuare tali sequestri ovvero coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazione. In sostanza sono stati aggiunti ai tradizionali soggetti esercenti il servizio postale anche coloro che offrono servizi telematici di comunicazione (internet service provider, gestori telefonici, enti certificatori di posta elettronica certificata, chat, messaggerie elettroniche) e tutti coloro che offrono un servizio di comunicazione elettronica, accessibile al pubblico attraverso qualunque tipologia di spedizione on line della corrispondenza.
La modifica della norma ha ampliato anche l'ambito oggettivo del materiale sequestrabile includendo anche le comunicazioni informatiche (57).
L'orientamento costante della giurisprudenza ha stabilito che l'art. 254 c.p.p. è norma speciale rispetto alla disciplina generale dei sequestri (58) e non soltanto perché tutelata dall'art. 15 della Costituzione e dall'art. 8 Cedu, ma anche perché applicabile al sequestro di corrispondenza ''in corso di spedizione'' e quindi a tutta la corrispondenza giacente presso gli uffici postali o, per quella informatica, presso gli internet service provider, alle cassette postali o durante il recapito della posta tramite il portalettere.
La specialità della norma si evidenzia anche dalla individuazione rigorosa dei soggetti legittimati a disporre il sequestro. La presenza della riserva di giurisdizione esclude che la polizia giudiziaria possa di iniziativa disporre l'acquisizione e l'apertura anche in presenza di posta elettronica.
Ciò non significa però che la materiale apprensione della corrispondenza debba essere eseguita esclusivamente dall'autorità giudiziaria essendo prevista la possibilità di delega ad ufficiali di polizia giudiziaria tenuti a consegnare all'autorità delegante gli oggetti sequestrati senza aprirli o alterarli e senza prendere conoscenza del loro contenuto.
A questo proposito si deve sottolineare la particolare delicatezza della corrispondenza elettronica che per una sua caratteristica tecnica non solo è ad alto rischio di alterazione ma non viaggia e non si conserva ''chiusa'' in un plico o in una busta bensì è per lo più rinvenibile ''aperta'' e conoscibile soprattutto nell'''oggetto'' anche soltanto con la semplice apertura del file che la contiene. Nei casi di urgenza e nell'impossibilità di avvisare tempestivamente l'Autorità Giudiziaria, in presenza di posta elettronica, è possibile ricorrere ex art. 353, 3º co., c.p.p. al cosiddetto fermo postale che in tal caso sarà meramente elettronico con l'effetto di trattenere la corrispondenza per una durata massima di 48 ore trascorse le quali, se il pubblico ministero non l'ha sequestrata o acquisita in copia, verrà inviata al destinatario.
Il sequestro della posta elettronica deve essere tenuto distinto con la captazione da remoto ed in tempo reale del flusso di dati, comprendente anche la posta elettronica, realizzabile mediante il diverso meccanismo dell'intercettazione telematica (59) regolamentato dall'art. 266 bis c.p.p.
In epoca antecedente alla modifica normativa, la dottrina aveva lamentato il ricorso generalizzato a provvedimenti di sequestro di un intero computer o dell'insieme del sistema informatico rilevando come fosse sufficiente intervenire con provvedimenti mirati su specifiche tracce informatiche (60). Questa impostazione è stata poi condivisa anche dalla giurisprudenza che ha sottolineato la necessità di evitare l'indiscriminata sottoposizione a sequestro probatorio di un intero hard disk o server avente spesso un contenuto in gran parte riservato e documenti non attinenti ai fatti (il computer era di una giornalista) e di adottare invece provvedimenti atti ad evitare interventi eccessivamente intrusivi (61).

(57) Aterno-Cajani-Costabile-Mattiucci-Mazzaraco, in *Manuale*, cit., 289 ss.
(58) Cass. pen., 13-10-2009, n. 47009, *GDir*, 2010, n. 6, 76.
(59) Luparia, *La ratifica della Convenzione di Cybercrime del Consiglio d'Europa. I profili processuali*, cit., 717.
(60) Cisterna, *Ricerca da circoscrivere a singoli soggetti per evitare ''irragionevoli intrusioni''*, *GDir*, 2007, n. 31, 57; Costabile, *Scena criminis, documento informatico e formazione della prova penale*, *DII*, 2005, 534.
(61) Cass. pen., 31-5-2007, n. 40380, *CP*, 2008, 11, 4276.

8. (Segue). *Il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni ex art. 254 bis c.p.p.*
L'art. 254 bis c.p.p. (modificato dalla legge n. 48/2008 di Ratifica della Convenzione di Budapest del 2001) disciplina il quomodo dell'acquisizione dei dati descrivendo con precisione il metodo e le procedure da adottare in caso di sequestri probatori o comunque acquisizioni di dati presso i fornitori di servizi informatici, telematici e di telecomunicazioni.
La norma è stata voluta allo scopo di indicare una metodologia di acquisizione e prevede indicazioni di principio allo scopo di garantire l'acquisizione mediante copia dei dati su adeguato supporto con una

procedura che sia in grado di assicurare la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.
Al contempo, la norma impone, al fornitore dei servizi destinatario del provvedimento cautelare, una conservazione e una protezione adeguata dei dati e delle informazioni originali anche oltre i termini di conservazione e di cancellazione previsti dalla legge (62).
La norma è nata dalla preoccupazione del Legislatore e dall'esigenza di tutela della prova da possibili incidenti tecnici o eventi illeciti, che frequentemente possono capitare in ambiente informatico. A volte, in occasione di alcune indagini, si è scoperta una certa facilità di manipolazione dei dati, una acquisizione dei dati di traffico senza alcuna traccia delle operazioni di accesso, oppure di tabulati consegnati all'Autorità giudiziaria carenti sotto il profilo della conformità con il dato originale.
Sotto il profilo soggettivo la norma si riferisce ai fornitori di servizi informatici, telematici e di telecomunicazione, pertanto devono escludersi tutti gli altri soggetti che non rientrano in questa categoria come ad esempio le aziende private, le banche, gli enti pubblici e la pubblica amministrazione.
A quest'ultimi, in caso di sequestro di dati informatici, potranno essere applicate le regole ordinarie disciplinate dagli artt. 253 ss. c.p.p. e quelle sulla conservazione delle cose deperibili anch'esse aggiornate secondo i principi della Convenzione di Budapest del 2001 (art. 260 c.p.p. così come modificato dalla legge n. 48/2008).
Con l'applicazione dell'art. 254 bis c.p.p. si possono acquisire ad esempio, con provvedimento di sequestro e con le garanzie di cui sopra, tutti i file di log di navigazione sul web se e in quanto ancora esistenti e non cancellati, garantendo al tempo stesso sia la regolare fornitura del servizio di Internet Service Provider (che può continuare a svolgere le normali attività nonostante il provvedimento acquisitivo), sia le esigenze di indagine, sia l'adempimento degli obblighi derivanti dalla normativa sulla data retention (d.lg. n. 109/2008 e art. 132 del d.lg. n. 196/2003 sulla cancellazione da parte del gestore dei dati nei casi e nei tempi previsti dalla legge).
La norma appare molto preziosa ai fini investigativi (anche difensivi) perché prevede in sostanza che un provvedimento di sequestro non può privare definitivamente i fornitori dei dati relativi ad un utente. Deve essere garantita la regolarità della fornitura e anche il dato originale che deve essere conservato e protetto dal fornitore.
Ciò consentirà in futuro l'accesso agli stessi dati anche da parte di altri soggetti legittimati e interessati, nonché eventuali indagini difensive.
In materia di acquisizione e conservazione di dati informatici presso terzi vi è una prima sentenza del Tribunale del Riesame di Roma 8-7-2008, inedita, a cui è seguita una pronuncia della Suprema Corte di Cassazione, avente ad oggetto una richiesta di sequestro erroneamente fondata sull'art. 254 bis c.p.p. in quanto in realtà rivolta ad un istituto bancario che presso i propri server conservava il file delle email in formato ''.pst'' delle cartelle outlook dell'indagato (istituto bancario quindi e non fornitore di servizi informatici o di telecomunicazione come previsto dall'art. 254 bis c.p.p.) (63).

(62) Per una approfondita analisi degli aspetti processuali, si veda, L. Luparia, *La ratifica della convenzione sul cyber crime del Consiglio d'Europa. I profili processuali*, cit., 717 ss.; Marafioti, *Digital Evidence e processo penale*, *CP*, 2011, 4509; Monti, *La nuova disciplina del sequestro informatico*, in AA.VV., *Sistema penale e criminalità informatica*, Milano, 2009, 210; per una trattazione specifica dell'articolo in commento si consenta il rinvio a Aterno, *sub* art. 8 *della legge 8-3-2008*, *n. 48*, in AA.VV., *Cybercrime, responsabilità degli enti*, *prova digitale*, Padova, 2009, e Aterno-Cajani-Costabile-Mattiucci-Mazzaraco, in *Manuale*, II, 2011, cit., 282 e 489.
(63) Cass. pen., sez. II, 13-3-2009, n. 11135, *GDir*, 2009, n. 17, 84 ss.

9. *Atti ripetibili e atti irripetibili.*
Sull'alterabilità del dato informatico si discute da tempo (64) ed è chiaro che le strategie di parte, le esigenze di urgenza del pubblico ministero e della difesa condizionano molto la scelta sul tipo di accertamento da effettuare. Le diverse parti processuali devono necessariamente effettuare un'analisi attenta delle due strade che si pongono loro di fronte: procedere ai sensi dell'art. 359 c.p.p. ad operazioni ripetibili oppure procedere con modalità irripetibili ai sensi dell'art. 360 c.p.p. dando però avviso dell'avvio delle operazioni alle altre parti.
L'esigenza di preservare l'integrità dei dati per consentire eventualmente ulteriori accertamenti, consulenze difensive o perizie future comporta che le acquisizioni e le analisi forensi vengano effettuate attraverso accertamenti tecnici ripetibili grazie all'ausilio di particolari strumenti informatici hardware e software i quali se correttamente usati (65), consentono di ripetere l'accertamento ogni volta che ve ne sia la necessità senza che l'elemento di prova venga alterato.
Le tecniche di acquisizione tipiche della forensics consentono tale ripetibilità in quanto determinano una ''cristallizzazione'', un ''congelamento tecnico'' del supporto informatico che anche dopo la sua ''clonazione'' per mezzo della già ricordata bit stream image (cfr. par. 1), conserverà tutti gli elementi necessari per un'approfondita e completa analisi investigativa.
Salvo in alcune particolari situazioni che possono dipendere anche dalla tipologia di strumenti informatici da acquisire (es.: cellulari, smartphone, ipad,

ipod, tablet, ecc.) l'acquisizione dell'elemento probatorio digitale può avvenire senza dover effettuare un accertamento irripetibile ex art. 360 c.p.p. che a volte comporta una discovery non gradita all'accusa e dall'altra l'inserimento dei verbali degli atti irripetibili nel fascicolo del dibattimento ex art. 431, lett. *c*), c.p.p. con tutte le conseguenze del caso spesso non gradite alla difesa.

Generalmente quindi non vi è una prevalenza tecnica dell'uno o dell'altro tipo di accertamento. In questa sede si cercherà di approfondire alcune disposizioni normative strettamente correlate alla fase di acquisizione e di accertamento delle prove digitali senza prendere una posizione che, ad avviso di chi scrive non può essere presa senza considerare le circostanze concrete e fattuali.

Non vi è dubbio che il Legislatore nel disciplinare gli artt. 359 c.p.p. e 360 c.p.p. poteva essere più chiaro e preciso. Nella disciplina codicistica che descrive i due accertamenti vi è una forte confusione terminologica. Mentre l'art. 359 c.p.p. riconosce al pubblico ministero la facoltà di nominare ed avvalersi di consulenti tecnici ove intenda provvedere ad accertamenti, rilievi segnaletici, descrittivi o fonografici e ogni altra operazione tecnica per la quale sono necessarie specifiche competenze, l'art. 360 c.p.p. opera un rinvio all'articolo precedente senza menzionare ad esempio i cosiddetti ''rilievi'' e dedicando una specifica regolamentazione ai soli «accertamenti tecnici non ripetibili».

È pacifico e costante in giurisprudenza che con il termine «rilievi» si intende indicare un'attività di mera osservazione, individuazione ed acquisizione di dati materiali, mentre gli «accertamenti» comportano un'opera di studio critico, di elaborazione valutativa ovvero di giudizio di quegli stessi dati. La Corte di Cassazione ha puntualizzato che il concetto di accertamento non comprende la constatazione o la raccolta dei dati materiali pertinenti al reato o alla prova (essi infatti si esauriscono nei semplici rilievi), ma riguarda lo studio e la elaborazione critica degli stessi (66). Ciò detto, è di tutta evidenza che l'irripetibilità dei rilievi e più specificatamente l'acquisizione o meglio l'apprensione dei supporti sottoporre ad analisi forense, non implica necessariamente l'irripetibilità dell'accertamento tecnico (67). Ciò si verifica soprattutto nei casi in cui operando sul reperto con modalità irripetibili sarà in futuro ancora tecnicamente possibile sottoporre i dati ivi contenuti alle operazioni necessarie per giungere con ragionevole approssimazione alla veritàprocessuale (68). Ciò può accadere per esempio in caso di prelevamento fisico di un server da un centro elaborazione dati di un soggetto terzo non indagato (si pensi ad esempio ad un internet service provider) in considerazione del fatto che tale operazione di asporto è di tipo irripetibile mentre le operazioni successive di acquisizione informatica del contenuto del server possono essere effettuate anche con modalità e tecniche ripetibili.

L'accertamento tecnico non ripetibile ai sensi dell'art. 360 c.p.p., pur talvolta utilizzato da alcuni organi inquirenti anche in occasione di grandi processi, non consente una buona difesa soprattutto in presenza di numerosi supporti sotto sequestro, degli stretti tempi in cui le operazioni devono essere svolte e soprattutto a causa della modifica reale e concreta del supporto sul quale si compie l'accertamento tecnico. Tale ultima circostanza può comportare un pregiudizio irreparabile per qualsiasi delle parti processuali in quanto in caso di errori compiuti nella fase di acquisizione e/o di analisi, ad esempio a sfavore dell'imputato, sarà ben difficile anche per un buon consulente tecnico risalire all'originarietà di un dato ormai compromesso.

Come già accennato precedentemente può accadere che circostanze fattuali o tecniche rendano i dati informatici rinvenuti sulla scena criminis alterabili non soltanto nel loro contenuto, ma anche nella loro struttura interna (es.: si modificano i cosiddetti metadati che contengono le specifiche tecniche di un file ed altre informazioni spesso molto utili alla ricostruzione dei fatti; oppure si rinvengano telefoni cellulari o smartphone). In questi casi è necessario svolgere attività di acquisizione dati con modalità irripetibili e quindi ai sensi dell'art. 360 c.p.p. comunicando alle altre parti processuali (difensore e indagato soprattutto) l'inizio delle attività, il luogo dove esse avranno inizio, ed eventuali consulenti nominati (69).

La prassi ormai consolidata delle forze di polizia e delle procure italiane si sta orientando verso l'acquisizione delle tracce informatiche con modalità ripetibili.

Recentemente alcune importanti sentenze di legittimità hanno affrontato il tema sotto diversi profili.

In particolare nell'ipotesi di lettura del contenuto di un personal computer (e successiva analisi) effettuata dalla polizia giudiziaria in assenza dei difensori, ove venga accertata l'assenza di alterazione del disco informatico, la Suprema Corte ha ritenuto che si è in presenza di una attività ripetibile. I giudici di legittimità hanno infatti stabilito che in siffatto caso non si dà luogo ad un accertamento tecnico irripetibile in quanto la lettura dell'''hard disk'' di un computer sequestrato, è attività di polizia giudiziaria volta, anche con urgenza, all'assicurazione delle fonti di prova ed è di natura ripetibile (70).

Si deve porre in evidenza però l'importante passaggio della sentenza sopra citata in merito proprio all'accertamento dell'assenza di alterazione dell'hard disk.

Ciò che sposta il confine tra atto ripetibile e irripeti-

bile è l'attenta acquisizione dei dati dal supporto originale e la possibilità di provare successivamente a livello scientifico che i dati della copia effettuata sono identici (in senso informatico) a quelli originali e che il supporto originale nel frattempo o durante le operazioni non è stato modificato o alterato. La Corte di Cassazione ha, a questo proposito ritenuto che non rientra nel novero degli atti irripetibili l'attività urgente ed immediata di estrazione di copia di un ''file'' da un computer oggetto di sequestro, dal momento che essa non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcuna alterazione dello stato delle cose tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata (*rectius*: dovendo essere sempre assicurata) la riproducibilità anche in futuro delle informazioni identiche a quelle contenute nell'originale e sempre che le operazioni siano state eseguite da personale qualificato (71).

Quest'ultimo orientamento, nel caso concreto, è fondato ed è corretto se si fonda sulla circostanza che il personal computer, dal quale con urgenza è stato estrapolato un file ''d'interesse'' investigativo, deve essere immediatamente posto sotto sequestro in modo da garantire sempre (anche alla difesa) la ripetibilità dell'operazione al fine di verificare la produzione del medesimo risultato finale.

Ad oggi e sotto il profilo scientifico ciò che garantisce che la copia di un file o di un supporto è uguale all'originale e comprova l'assenza di alterazioni nei files (anche soltanto nei metadati) è la procedura tecnica di hashing di cui si è già parlato nei par. 1 e 3 ed ai quali si rinvia.

Recentemente anche la Corte di Cassazione (per la prima volta in una sede giudiziaria), su impulso della difesa, si è pronunciata sull'esperibilità delle procedure di hashing al fine di verificare l'integrità e la conformità all'originale del dato informatico sequestrato e conservato in copia su un apposito supporto (nella specie cd-rom). I giudici di legittimità hanno ritenuto che il tema fosse una questione di merito da risolversi in tale sede, potendosi in sede di legittimità esclusivamente delibare solo se gli accorgimenti adottati dalla polizia giudiziaria delegata siano o meno idonei in astratto a tutelare le finalità indicate dal legislatore negli artt. 247, co. 1 bis, e 354, 2º co., c.p.p. come modificati dalla legge n. 48/2008 di ratifica della Convenzione del Consiglio d'Europa sul cybercrime.

(64) Per i primi commenti si vedano i riferimenti dottrinali indicati nella nota 1 del par. 1.

(65) Con riguardo alla corretta esecuzione e alla qualifica dell'operatore tecnico, si veda Cass. pen., sez. I, 26-2-2009, n. 11863, *CED*, 243922, secondo la quale l'estrazione dei dati contenuti in un supporto informatico, se eseguita da personale esperto in grado di evitare la perdita dei medesimi dati, costituisce un accertamento tecnico ripetibile.

(66) Così Cass. pen., sez. I, 14-3-1990, n. 301, *CED*, 183648, si veda altresì tra le altre Cass. pen., sez. V, 20-11-2000, n. 11866, *GDir*, 2001, 105 ss.

(67) Per una attenta analisi di queste tematiche si veda E. Aprile, *Le indagini tecnico scientifiche: problematiche giuridiche sulla formazione della prova penale*, *CP*, 2003, 4034 ss.

(68) Cass. pen., sez. I, 31-10-1994, n. 10893, *CED*, 200176. Si riporta la relativa massima: «Poiché il concetto di accertamento non comprende la constatazione o la raccolta dei dati materiali pertinenti al reato o alla sua prova, i quali si esauriscono nei semplici rilievi, ma riguarda piuttosto lo studio e la elaborazione critica dei medesimi, la irripetibilità dei rilievi, più specificamente dell'acquisizione dei dati da sottoporre ad esame non implica necessariamente la irripetibilità dell'accertamento, quando l'esito di una prima indagine non appaia, ad avviso del giudice che procede, del tutto convincente e sia ancora tecnicamente possibile sottoporre quei dati alle operazioni necessarie al conseguimento di risultati attendibili».

(69) Cass. pen., S.U., 17-10-2006, n. 41281.

(70) Cass. pen., sez. I, 25-2-2009, n. 11503, *CED*, 243495.

(71) Cass. pen., sez. I, 5-3-2009, n. 14511, *CED*, 243150.

10. *Strumenti investigativi informatici e mezzi di ricerca della prova atipici: il ''pedinamento informatico'' tramite sistema GPS.*

L'osservazione dei movimenti di un soggetto attraverso un sistema di ricezione satellitare (cosiddetto Global position system), chiamato anche ''pedinamento informatico'', è utilizzata molto spesso dalle forze dell'ordine per controllare da remoto i movimenti di un personaggio sospetto o sotto indagine.

Sono ormai numerose le pronunce della giurisprudenza sull'utilizzo a scopo investigativo di questi sistemi occultati nelle autovetture e controllabili da remoto. Negli ultimi tempi si segnala anche una frequente utilizzazione del sistema di geolocalizzazione su apparati mobili cellulari e in special modo sugli smartphone (72).

Il problema è cercare di capire quale disciplina giuridica deve applicarsi a questo sistema di controllo a distanza dei movimenti di un individuo.

La particolarità della geolocalizzazione o ''positioning'' è l'osservazione in tempo reale del movimento del soggetto ''sul'' quale in maniera occulta è stato installato l'apparecchio (hardware o software) che rileva la posizione e le coordinate spazio-temporali (73) relative agli spostamenti.

È bene precisare che ci troviamo questo sistema è diverso dalla localizzazione attraverso le celle dei tabulati telefonici ovvero quando in un momento successivo al sequestro di un apparato informatico (es. smartphone) si acquisiscono direttamente su di esso le coordinate del traffico telefonico/telematico effettuato e gli altri elementi idonei alla localizzazione. In quest'ultimi casi si effettua una ricostruzione ex post degli spostamenti del soggetto attraverso software e hardware di computer forensic che analizzano le tracce dei sistemi interni di georeferenziazio-

ne raffigurandole direttamente su mappe geografiche in modo tale da fornire agli inquirenti o al giudice un'esatta ricostruzione storico -geografica degli spostamenti .

Altra ipotesi di geolocalizzazione è quella di cui parleremo più avanti ovvero la ricostruzione della posizione di un soggetto assunta a ritroso nel tempo attraverso l'analisi di un tabulato e delle celle telefoniche agganciate dal sistema.

È di tutta evidenza comunque che in tutti i casi sopra esaminati il sistema è in grado di captare soltanto la posizione e non anche eventuali comunicazioni che tra soggetti (74).

Si tratta di un metodo di indagine per certi versi invasivo che in parte va ben oltre ciò che può fare l'agente di polizia nel consueto pedinamento ''fisico'' soprattutto perché è in grado di rilevare ogni spostamento dell'individuo anche quando entra in luoghi privati all'interno dei quali non potrebbe estendersi il pedinamento normale.

In materia di geolocalizzazione l'orientamento della Cassazione è pacifico nel ritenere che il tracciamento tramite sistema satellitare degli spostamenti di un individuo, benché comporti un controllo non poco invasivo a carico del soggetto medesimo, non è in alcun modo assimilabile alla attività di intercettazione, prevista dagli artt. 266 ss. c.p.p. e non necessita quindi di alcuna autorizzazione preventiva da parte del giudice per le indagini preliminari (75). Alla ricerca di una similitudine con altri mezzi di ricerca della prova, la giurisprudenza ha ritenuto che la localizzazione mediante sistema satellitare costituisce una forma di pedinamento o comunque una modalità, tecnologicamente caratterizzata, di ''pedinamento'' e di osservazione di polizia giudiziaria che quindi non necessita di alcuna autorizzazione preventiva da parte del giudice per le indagini preliminari rientrando tra le cosiddette prove atipiche (76) di cui all'art. 189 c.p.p.

In particolare, secondo l'orientamento di parte della giurisprudenza non sarebbe necessario neanche il decreto del pubblico ministero in quanto tale attività di geolocalizzazione rientrerebbe nei mezzi di ricerca della prova cosiddetti atipici o innominati attribuiti alla competenza della polizia giudiziaria (cfr. artt. 55, 347, 370 c.p.p.). e non troverebbe comunque applicazione il disposto dell'art. 15 Cost., che tutela le comunicazioni interpersonali (77) in considerazione del fatto che tale strumento non le intercetterebbe.

Secondo un'altra pronuncia della Corte di Cassazione (78) l'attività di geoposizionamento sarebbe un'attività investigativa atipica assimilabile al pedinamento ma ripetibile in quanto i risultati possono entrare nella valutazione probatoria del giudice attraverso la testimonianza degli ufficiali di polizia giudiziaria e non hanno il carattere degli ''atti non ripetibili'' e quindi non vanno inseriti nel fascicolo del dibattimento.

La prima pronuncia sulla geolocalizzazione in tempo reale attraverso il controllo del telefono cellulare mobile (79) ha ritenuto, conformemente all'orientamento costante, che la localizzazione delle persone attraverso l'apparato cellulare in possesso delle stesse non necessita di autorizzazione giudiziale, risolvendosi in una sorta di pedinamento satellitare e non interferendo sulla libertà e segretezza delle comunicazioni.

Se l'orientamento dei giudici di legittimità è condivisibile nel punto in cui non ritiene che la geolocalizzazione sia un'intercettazione telematica, appare meno spiegabile il silenzio argomentativo relativo all'affievolimento del diritto costituzionale della libertà di circolazione (art. 16 Cost.) determinato da nuove tecniche investigative e da norme processuali ormai datate e forse bisognose di modifiche.

Fuori dalle ipotesi di georeferenziazione si pone il diverso caso dell'analisi delle celle telefoniche o telematiche (Bts) (80) di un operatore telefonico agganciate dal telefono mobile. Questi dati di traffico indicati dall'art. 3 del d.lg. n. 109/2008 e dal d.lg. n. 196/2003 e conservati per le finalità di cui all'art. 132 c. privacy presuppongono l'esistenza di una comunicazione in atto tra più soggetti o comunque una comunicazione telematica che produce il dato di traffico che viene conservato.

Ai fini della loro acquisizione, si applica quindi la disciplina dettata dall'art. 132 del d.lg. n. 196/2003 (c. privacy), il quale, al 3º co., stabilisce che i dati relativi al traffico «sono acquisiti presso il fornitore con decreto motivato del pubblico ministero».

La loro acquisizione da parte delle forze di polizia nell'espletamento dei compiti disciplinati dall'art. 55 c.p.p. non può, pertanto, avvenire con modalità difformi da quelle specificatamente previste dalla legge.

Tornando allo strumento della geolocalizzazione e all'orientamento ormai costante della giurisprudenza che gli attribuisce natura di mezzo di ricerca atipico della prova con la garanzia debole prevista dall'art. 189 c.p.p., ci si domanda se non sia il momento in questi casi di mostrare particolare attenzione all'esigenza di introdurre maggiori garanzie.

Questi strumenti investigativi altamente tecnologici sono capaci di ripetere e di effettuare ''in serie'', massivamente, automaticamente e, in teoria, senza limiti di tempo, un'invasione nella sfera privata dell'individuo senza neanche che vi sia l'intervento del giudice per le indagini preliminari e talvolta neanche del pubblico ministero.

È ben vero che il pedinamento tradizionale è per altri versi invasivo perché consente all'agente di individuare con precisione particolari che invece sfuggono al pedinamento satellitare ma la facilità di utilizzo del mezzo, la possibilità concreta che a farlo sia un solo

agente di polizia in grado di installare e effettuare un grande numero di pedinamenti satellitari durante o fuori l'orario di servizio, impone una riflessione sull'opportunità di prevedere almeno il decreto del pubblico ministero.

A questo proposito vale la pena brevemente di richiamare alcuni passaggi di una recente pronuncia della Corte europea dei diritti dell'uomo in materia di geolocalizzazione satellitare e violazione della Cedu.

Nel ricorso ''Uzun contro la Repubblica federale di Germania'' del 2-9-2010, inoltrato alla Corte ai sensi dell'art. 34 della Convenzione Europea dei diritti dell'uomo da un cittadino tedesco, si ipotizzava che durante le indagini, le misure di sorveglianza cui era stato sottoposto, in particolare l'osservazione via GPS e l'uso dei dati così ottenuti nel processo penale contro di lui, avevano violato il suo diritto al rispetto della vita privata riconosciuto dall'articolo 8 della Convenzione.

La Corte ha riconosciuto che i mezzi tecnici in questione ricomprendono metodi di sorveglianza che non sono né visivi né acustici e che sono usati, in particolare, ''per individuare dove si trova l'autore di un reato'', ma ha specificato anche che il codice tedesco prevede alcune norme che tipizzano gli strumenti adottati e che proprio per questo l'utilizzo può considerarsi legittimo.

Nell'esaminare se la legge nazionale tedesca contenesse garanzie adeguate e effettive contro gli abusi, la Corte ha ulteriormente osservato che effettivamente, all'epoca dei fatti, non esisteva un limite fissato dalla legge per la durata di tale monitoraggio ma che successivamente un termine fisso è stato previsto dalla legge nella misura in cui la sorveglianza sistematica di un sospettato ordinata da un pubblico ministero non può eccedere un mese e che ogni ulteriore dilatazione di tale termine può essere ordinata solo da un giudice.

Con riguardo ai motivi richiesti per ordinare la sorveglianza di un individuo via GPS, la Corte ha notato che, ai sensi del codice di procedura penale tedesco, tale sorveglianza può essere ordinata solo contro una persona sospettata di un reato di notevole gravità o, in circostanze molto limitate, contro una terza persona sospettata di essere in contatto con l'imputato ma soltanto se gli altri mezzi di individuazione dei luoghi in cui si trova l'imputato hanno minore prospettiva di successo o sono più difficoltosi.

La Corte ha ritenuto che il diritto interno tedesco prevede delle norme abbastanza rigorose per autorizzare la misura di sorveglianza in questione e che appare legittimo che il pubblico ministero sia in grado di ordinare la sorveglianza via GPS di un sospettato e di delegarla alla polizia ma nel rispetto dei limiti previsti dalla legge.

La Corte ha inoltre osservato anche che, a norma dell'art. 163 f § 4 del codice di procedura penale tedesco, che è entrato in vigore dopo che la sorveglianza via GPS del ricorrente era stata compiuta, la sorveglianza sistematica di un sospettato per una durata superiore a un mese deve effettivamente essere ordinata da un giudice e che pertanto per il futuro non sarebbe stato più sufficiente il provvedimento del solo pubblico ministero. In questo senso la Corte europea accoglie questo rafforzamento del diritto di un soggetto al rispetto della propria vita privata e del pari rafforza le garanzie contro eventuali abusi soprattutto con riferimento all'attivazione ingiustificata dello strumento nei confronti del medesimo soggetto in modo sistematico e ripetuto nel tempo.

(72) Nei casi che riguardano quest'ultimi, lo strumento sotto controllo è attivabile e disattivabile anche da remoto soprattutto nel caso in cui l'autorità giudiziaria abbia autorizzato le forze di polizia ad utilizzare sistemi di intrusione e di controllo dell'apparato informatico (v. paragrafo sul captatore informatico).
(73) Per uno dei primi commenti alla geolocalizzazione satellitare su autovettura si veda A. LARONGA, *L'utilizzabilità probatoria del controllo a distanza eseguito con sistema satellitare g.p.s.*, *CP*, 2002, 3050.
(74) Salva l'ipotesi di contemporaneo utilizzo di apparati tecnologici complessi attrezzati anche alla captazione del suono.
(75) Cass. pen., sez. V, 27-2-2002, n. 16130, *CED*, 221918.
(76) Cass. pen., sez. V, 7-5-2004, n. 24715, *CED*, 228731; si veda inoltre, Cass. pen., sez. IV, 29-1-2007, n. 8871, *CED*, 236112; Cass. pen., sez. IV, 1-3-2007, n. 887119; Cass. pen., sez. IV, 28-11-2007, n. 3017, *CED*, 238679.
(77) Cass. pen., sez. IV, 1-3-2007, n. 887119.
(78) Cass. pen., sez. VI, 11-12-2007, n. 15396, *CED*, 239638. Nello stesso senso, si veda, Cass. pen., sez. I, 9-3-2010, n. 9416, *CED*, 246774.
(79) Cass. pen., sez. I, 28-5-2008, n. 21366, *CED*, 240092.
(80) Base Transcelver Station.

11. (Segue). *L'appostamento informatico come mezzo di ricerca atipico della prova.*

È di tutta evidenza che le nuove tecniche di indagine ad alto livello tecnologico stimolano giurisprudenza e dottrina a cercare adeguate risposte nonostante i vecchi strumenti processuali a disposizione.

Nuove questioni giuridiche sorgono in relazione a questi nuovi metodi di indagine. Ad esempio, l'anonimato in rete costituisce un forte ostacolo ad ogni tipo di accertamento investigativo. Dietro anonimi indirizzi email o siti internet apparentemente senza ''proprietario'' si celano persone reali che sfruttano strumenti informatici in grado di rendere chiunque assolutamente anonimo.

Esistono tecnologie di contrasto basate a loro volta su programmi informatici nuovi e spesso studiati ed elaborati all'occorrenza. Ma queste nuove indagini come possono essere definite? E quali istituti giuridici possono essere coinvolti per garantire il rispetto delle norme a tutela dell'individuo?

Riuscire a tracciare e risalire all'indirizzo IP reale (e

quindi all'identificazione dell'utente) di un account di posta elettronica (oppure di un server o sito internet) chiaramente inventato o creato con false generalità dall'altra parte dell'emisfero è una intercettazione telematica ex art. 266 bis c.p.p. oppure un tracciamento equiparabile ad un appostamento di polizia giudiziaria o piuttosto ad una geolocalizzazione? A questa domanda cercheremo di rispondere poco più avanti non prima di aver fatto alcune necessarie premesse.

L'utilizzo a scopo illecito di email anonime create con account di fantasia su server allocati in paesi cosiddetti ''paradisi informatici'' rappresenta una costante in quasi tutte le più importanti indagini informatiche. I cosiddetti ''paradisi informatici'' per loro natura sono poco inclini a rispondere alle rogatorie internazionali. Sono frequenti i casi di soggetti che, in completo anonimato, compiono atti illeciti attraverso l'invio di posta elettronica senza correre il minimo rischio di essere rintracciati. Oggi è abbastanza semplice aprire un sito internet su un server collocato dall'altra parte del pianeta, ad esempio in Malesia o in Transnistria (81), con indirizzi email di fantasia offerti dal servizio e rimanere anonimo anche dopo uno scambio di email. Da un lato il titolare dell'account o del sito potrebbe addirittura a non rispondere mai alla posta che riceve proprio per il pericolo di essere localizzato ma limitarsi a pubblicare o diffondere il materiale, spesso illecito, che gli viene offerto. Dall'altro può utilizzare sistemi di anonimizzazione sicura nel caso in cui volesse rispondere e spedire email in tutta tranquillità. Senza arrivare a parlare di sistemi tipo Tor (82), si può raggiungere l'anonimizzazione perfetta (o quasi..) controllando il proprio account passando attraverso una serie di proxy e sempre leggendo le email sul web ovvero non commettendo mai l'errore di scaricarle in locale sul proprio computer personale (es. attraverso la configurazione dell'account su outlook o su altro sistema di posta) con la propria linea telefonica.

In questo modo né i cosiddetti metadati, né l'indirizzo IP (internet protocol) presenti nel corpo dell'e-mail inviata saranno sufficienti ad identificare l'autore dell'invio; l'unico ad essere identificato sarà soltanto il server che fa da tramite e che spesso è allocato in un paese straniero che non fornisce alcuna collaborazione e non ha particolari obblighi di legge in materia di data retention.

Senza temere di fornire indicazioni che potrebbero istigare al compimento di tali fatti e facendo riferimento alle informazioni che molto più semplicemente sono rinvenibili in rete con una semplice ricerca, è di tutta evidenza che esistono da tempo in commercio sistemi e applicazioni informatiche che consentono l'invio di email traccianti in grado di identificare il reale indirizzo IP del soggetto che utilizza una rete di telecomunicazioni altrimenti non tracciabile.

Occorre domandarsi se questi strumenti informatici di identificazione del reale utilizzatore di quell'account di posta sono dei sistemi di ''tracciamento'' o ''identificazione mediante appostamento informatico'' oppure vere e proprie intercettazioni telematiche che pertanto devono essere autorizzate anche dal giudice oltre che dal pubblico ministero.

Il primo e finora unico utilizzo di cui si è (pubblicamente) a conoscenza è quello che ha riguardato alcuni anni fa un'attività investigativa volta ad accertare l'autore di alcune condotte di diffamazione on line poste in essere attraverso un sito web di gossip italiani ma le cui ''pagine'' erano allocate su un server in Australia. Il fatto è stato oggetto di alcune pronunce giurisprudenziali del Tribunale di Milano (83) e della Corte di Appello di Milano, nonché recentemente della Suprema Corte di Cassazione (84).

Il soggetto agente utilizzava una rete di telecomunicazioni non tracciabile ed erano risultate vane diverse azioni investigative, autorizzate dal pubblico ministero, volte ad accertare l'IP del reale mittente.

Dopo l'emissione del decreto del pubblico ministero si decise di ricorrere pertanto all'invio di alcune e-mail cosiddette traccianti all'indirizzo che risultava abbinato alla gestione editoriale del sito di gossip.

L'email tracciante funziona più o meno nel modo seguente: all'interno del messaggio di posta viene inserito un codice ''html'', appositamente studiato dalla polizia giudiziaria per consentire il tracciamento elettronico della postazione utilizzata in sede di lettura (85).

Questa attività investigativa – caratterizzata più dalla staticità dell'appostamento che dalla dinamicità di un pedinamento – è stata ribattezzata dalla sentenza di primo grado del Tribunale di Milano ''appostamento informatico'' in quanto di per sé idonea a rivelare la posizione e l'individuazione di un utente sulla rete internet ed è stato escluso possa essere riconducibile ad una attività di intercettazione telematica (art. 266 bis, c.p.p.) per l'assenza di qualsivoglia captazione di flussi di comunicazione intercorsi tra due soggetti.

Il software include un elemento invisibile all'utente nel corpo dell'e-mail da inviare. Tale elemento (spesso un'immagine infinitesimale dello stesso colore dello sfondo dalle dimensioni di un singolo pixel) genera una richiesta ad un server.

Quando l'utente apre il messaggio ricevuto, a sua insaputa genera una richiesta al server da cui verrà prelevata l'immagine. Questa permette di tracciare l'indirizzo IP dell'utente e l'orario del ''contatto''.

Quando l'utente apre il messaggio ricevuto vengono restituite di nascosto alla polizia giudiziaria le informazioni relative all'account del destinatario, la data di apertura del messaggio nonché tutte le altre infor-

mazioni tecniche relative alla consegna del messaggio o all'apertura dell'allegato.
Inoltre, a seconda dei software, sarà possibile georeferenziare colui che ha aperto il messaggio (rispetto alla posizione presunta, ovvero tramite il proprio provider), o il momento in cui ha aperto l'allegato o cliccato su un link dell'email).
Nel caso sopra enunciato, all'esito del processo di primo grado, il Tribunale di Milano ha riconosciuto la liceità dell'azione investigativa (posta in essere con decreto del pubblico ministero), non potendo essere la stessa inquadrabile in una attività tipica dell'agente provocatore e nemmeno in una attività di intercettazione telematica bensì come un vero e proprio ''appostamento informatico'' da intendersi come mezzo di prova atipico ex art. 189 c.p.p. molto simile ad una osservazione di polizia giudiziaria con cognizione di informazioni utili all'identificazione.
Qui il sistema in uso è informatico ed è pertanto necessario analizzare nello specifico gli aspetti giuridici coinvolti. Ciò che viene tracciato dagli investigatori (e da coloro che adottano tale strumento informatico) è l'indirizzo Internet Protocol (IP) di connessione cosiddetto ''originario'' (sorgente) nonché la data e l'ora in cui è stata aperta l'email.
Nel caso specifico l'IP che viene comunicato di nascosto dal sistema stesso alla P.G. è il numero univocamente assegnato ad un'utenza telefonica nel momento in cui il PC collegato ad essa si connette alla rete internet anche se poi l'utente va a leggersi la posta sull'account di un sito dall'altra parte del mondo; nel caso in questione l'efficacia del software utilizzato è quella di tracciare l'IP del computer davanti al quale si trova il soggetto titolare dell'account. Successivamente, a seguito della richiesta dell'Autorità all'operatore telefonico ex art. 132 d.lg. n. 196/2003 (anche in seguito a rogatoria), l'IP verrà ''trasformato'' nell'utenza telefonica e nel nome del soggetto intestatario del servizio che quel giorno ha aperto quell'email ''dall'altra parte del mondo''.
Questo tipo di tracciamento è un mezzo di ricerca atipico della prova ? Siamo in presenza, ex art. 266 bis c.p.p. della cognizione di un flusso di comunicazioni informatiche ?
La questione non è di semplice soluzione. Un flusso di comunicazioni informatiche è un insieme di dati informatici di vario genere; ad esempio il flusso dei dati relativi ad una navigazione su siti internet in quanto intercorrente tra il computer che naviga e l'internet service provider che offre l'accesso alla rete; oppure il flusso di dati trasmessi da un servizio di chat o di messaggeria informatica sia verso i server del servizio sia verso l'internet service provider.
Se è vero che tra questi dati c'è anche l'IP [ad oggi spesso sempre diverso (86)] che viene assegnato fin dal primo momento della connessione (cosiddetto ''IP di origine''), è anche vero che quest'ultimo non è parte integrante del flusso di dati che costituiscono il contenuto della comunicazione (87). Non bisogna dimenticare che soltanto il contenuto di una comunicazione è giustamente tutelato dalle norme in materia di intercettazione. L'indirizzo IP costituisce soltanto l'elemento identificativo del soggetto che si connette alla rete. Non trova quindi molte argomentazioni ritenere di tutelare con la norma sulle intercettazioni telematiche la cognizione, seppur captata occultamente e con artificio, di un indirizzo IP di origine.
Non sembra essere giuridicamente corretta la riconducibilità della condotta investigativa sopra descritta ad un'attività sotto copertura o di provocazione perché manca del tutto l'attività illecita (scriminata) posta in essere dall'agente operante e inoltre, a ben vedere, con il ''tracciamento'' non si tenta di entrare in rapporto dialettico con l'indagato instaurando un contatto bensì si invia una finta email che il più delle volte è di tipo commerciale o contiene allegati ''accattivanti'' solo al fine di indurre il destinatario ad aprirla e ad infettarsi. Per usare un altro accostamento con la realtà investigativa e processuale, il sistema è simile all'ipotesi della telefonata della polizia giudiziaria o della scusa di una sigaretta o di un volantino per controllare da vicino l'identità e il viso del soggetto pedinato.
In tali casi non può esservi contestazione di attività sotto copertura né si rinviene giurisprudenza in tal senso.
Recentemente la Corte di Cassazione (88) si è pronunciata proprio in relazione al caso sopra esaminato e sembra aver dato ragione al tribunale di Milano perché ha ritenuto l'attività posta di essere dagli operanti su delega del pubblico ministero una mera attività di ricerca atipica della prova attraverso una tecnica di tracciamento informatico escludendo possa trattarsi di una intercettazione telematica ex art. 266 bis c.p.p.

(81) La Transnistria è uno stato ''indipendente di fatto'' non riconosciuto a livello internazionale, essendo considerato ufficialmente come parte della Repubblica di Moldavia: è governato da un'amministrazione autonoma. Osservatori della Comunità Europea, esprimendosi in merito alla preoccupante situazione dell'illegalità e del mancato controllo delle frontiere di questa regione alle porte dell'Unione, sono portati a ritenere che parte non irrilevante del flusso economico nazionale sia direttamente collegato ai traffici illeciti che derivano dal radicamento del crimine organizzato di mafie attive in tutta la Russia e dalla particolare posizione di passaggio di questo territorio per il flusso degli stupefacenti, delle armi e del contrabbando; questa situazione ha portato la stampa a definire il paese il ''buco nero d'Europa''. Fonte Wikipedia *http://it.wikipedia.org/wiki/Transnistria*.
(82) Tor (The Onion Router) è un sistema di comunicazione anonima per Internet. Tor protegge gli utenti dall'analisi del traffico attraverso una rete di onion router, gestiti da volontari,

che permettono il traffico anonimo in uscita e la realizzazione di servizi anonimi nascosti.
(83) T. Milano, VII sez. in composizione monocratica, 22-2-2010 (est. Barazzetta), inedita, vedi ampi stralci in ATERNO-CAJANI-COSTABILE-MATTIUCCI-MAZZARACO, in *Manuale*, 2012, cit., 462.
(84) Cass. pen., V, 7-6-2013 (in attesa del deposito delle motivazioni).
(85) Per le modalità tecniche dell'appostamento o tracciamento informatico si consenta il rinvio a ATERNO-CAJANI-COSTABILE-MATTIUCCI-MAZZARACO, in *Manuale*, 2012, cit., 462 ss.
(86) Almeno fino all'avvento dell'IPV6.
(87) Per la differenza tra IP di origine e IP identificativo del contenuto di una comunicazione si veda il provvedimento del Garante per la protezione dei dati personali, Sicurezza dei dati di traffico telefonico e telematico 17-1-2008 *G.U.* n. 30 del 5-2-2008, doc. web n. 1482111.
(88) Cass. pen., sez. V, 7-6-2013, n. 12180 ,che ha ritenuto come non costituisce una intercettazione di un flusso di comunicazioni l'attività che si assume concretamente realizzata dagli investigatori (con decreto del P.M.) e consistita nella verifica (non in tempo reale) degli identificativi IP di coloro che avevano avuto accesso ai siti d'interesse come meri fruitori ovvero come soggetti che aggiornavano il contenuto, e nell'invio di una comunicazione via email con uno script all'interno che ha catturato il reale IP utilizzato dal soggetto che gestiva il sito in questione.

12. (Segue). *Il captatore informatico e la cosiddetta Remote Forensics: un trojan per la captazione occulta da remoto del contenuto di un sistema informatico.*

Sempre più di frequente la criminalità utilizza strumenti informatici (hardware e software) in grado di far perdere le tracce dei delitti commessi. Le forze dell'ordine dal canto loro affinano le indagini e ricorrono alle nuove tecnologie per il contrasto delle condotte criminose.

Tra i nuovi strumenti utilizzati dalla criminalità informatica per disperdere nel cyberspazio il materiale illecito e le tracce del proprio operato, si pone il cosiddetto cloud computing. La cosiddetta ''nuvola'', è un nuovo ''spazio informatico'' e costituisce una grande risorsa per aziende e privati ma per la sua natura e struttura tecnica viene sfruttato anche per scopi illeciti. In una eterna rincorsa tra utilizzo criminoso delle tecniche informatiche e investigazioni altamente specializzate, le forze dell'ordine e la magistratura tentano di stare al passo dei criminali attraverso strumenti tecnologici spesso ai limiti delle garanzie previste dalla legge ma utilizzando talvolta gli stessi mezzi invasivi della riservatezza utilizzati dagli hackers.

L'acquisizione occulta on line da remoto del contenuto digitale di un supporto informatico collegato alla rete Internet è uno di questi metodi con i quali, tra le altre cose è possibile entrare, non senza difficoltà, in ogni spazio informatico d'interesse investigativo.

Ora il punto è chiedersi se vi sono norme che legittimano o potrebbero legittimare l'utilizzo di questa tecnologia.

Cercheremo di rispondere a questa domanda anche alla luce di una pronuncia giurisprudenziale di legittimità (89) che ha affrontato il problema.

Il fatto oggetto della sentenza della Cassazione trae origine da alcune indagini per associazione a delinquere di stampo mafioso e all'utilizzazione di un captatore informatico (software virus trojan) (90) disposto con decreto di acquisizione di atti ai sensi dell'art. 234 c.p.p., emesso dal pubblico ministero.

Il decreto aveva ad oggetto l'acquisizione in copia della documentazione (informatica) memorizzata all'interno del personal computer in uso ad uno degli imputati e installato presso alcuni uffici Comunali.

L'atto, pur autorizzando una mera acquisizione in copia degli atti, non presupponeva un'attività di intercettazione di comunicazioni informatiche ai sensi degli artt. 266 bis ss. c.p.p. e tale richiesta non fu portata all'attenzione del giudice per le indagini preliminari. Invero, il decreto disponeva la registrazione non solo dei files esistenti, ma anche dei dati inseriti in futuro nel personal computer, in modo da acquisirli periodicamente. Le concrete modalità esecutive del decreto, consistite nell'installazione, all'interno del sistema operativo del personal computer, di un captatore informatico erano in grado di memorizzare i files già esistenti e di registrare in tempo reale tutti i files elaborandi, innescando in tal modo un monitoraggio occulto e continuativo del sistema informatico.

Il problema che la Cassazione ha affrontato fu di stabilire se l'attività captativa fosse o meno un'attività di intercettazione telematica. La Corte di Cassazione nelle motivazioni, non ha ritenuto che questa captazione fosse un'attività di intercettazione telematica ex art. 266 bis c.p.p. in quanto la registrazione non avrebbe avuto ad oggetto «un flusso di comunicazioni» presupponente un dialogo con altri soggetti, ma «una relazione operativa tra microprocessore (??, ndr.) e video del sistema elettronico» ovvero «un flusso unidirezionale di dati». Il decreto del pubblico ministero, hanno precisato i giudici di legittimità, si era limitato a disporre che, ad opera della polizia giudiziaria, fossero estrapolati sia i dati già formati e contenuti nella memoria del personal computer in uso ad uno degli imputati sia quelli che in futuro sarebbero stati memorizzati. La Corte ha anche chiarito che per flusso di comunicazioni deve intendersi la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un ricevente, da un soggetto ad altro, ossia il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici, non potendosi ritenere intercettazione di un flusso di comunicazioni la captazione di un'elaborazione del pensiero e la sua esternazione in scrittura su di un personal computer oppure mediante simboli grafici apposti su

un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura.
Secondo la Suprema Corte, pertanto, l'attività di captazione in questione deve essere ricondotta nel concetto di ''prova atipica'', sottratta alla disciplina prescritta dagli artt. 266 ss. c.p.p., con conseguente e pacifico utilizzo dei risultati. La Corte ha risposto anche ad altre eccezioni ovvero ha ritenuto, che l'attività captativa non avesse violato né l'art. 14 Cost. né l'art. 15 Cost.
Il personal computer, infatti, si trovava nella locale sede di un ufficio pubblico comunale, ove sia l'imputato sia gli altri impiegati avevano accesso per svolgere le loro mansioni e ove potevano fare ingresso, sia pure in determinate condizioni temporali, il pubblico degli utenti e il personale delle pulizie, insomma una comunità di soggetti non particolarmente estesa, ma nemmeno limitata o determinabile a priori in ragione di una determinazione personale dell'imputato.
Nel caso di specie non poteva essere invocata la tutela costituzionale della riservatezza della corrispondenza e in genere delle comunicazioni, giacché quanto riprodotto in copia, non era un testo inoltrato e trasmesso col sistema informatico privato e personale, ma ''soltanto predisposto per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario''.
Non si è posto neanche il problema circa l'applicabilità della disciplina prevista per gli accertamenti tecnici irripetibili, atteso che l'attività di riproduzione dei files memorizzati non aveva comportato l'alterazione, né la distruzione dell'archivio informatico, rimasto immutato, quindi consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria. Si era trattato di un'attività sempre reiterabile, alla cui esecuzione non era necessaria la partecipazione del difensore, poiché la stessa poteva essere compiuta una seconda volta se solo si fosse poi approdato ad uno sviluppo dibattimentale del procedimento.
Sotto il profilo della prova atipica e della sua formazione la Corte ha altresì escluso la violazione della disciplina di cui all'art. 189 c.p.p., in quanto la mancata acquisizione in contraddittorio della prova documentale estrapolata dal personal computer era dipesa dalla scelta difensiva del rito abbreviato, e la prescrizione, ex art. 189 c.p.p., che impone al giudice di procedere in contraddittorio tra le parti riguarda l'assunzione delle fonti di prova e non dei mezzi di ricerca della prova.
Tale decisione della Suprema Corte è stata aspramente criticata (91) in quanto ha dimenticato e lasciato irrisolti molteplici aspetti.
Appare difficile smentire che siffatta attività di captazione da remoto attraverso un software trojan autorizzato dal pubblico ministero non sia un'intercettazione di comunicazioni informatiche o telematiche. Il personal computer per poter trasmettere dati all'organo di polizia era necessariamente connesso alla rete internet tramite Internet serve provider (92) e tra i dati captati da remoto vi era certamente, anche in parte, il flusso di dati relativi alla navigazione su Internet ovvero a comunicazioni effettuate tra il personal computer e l'Internet serve provider. Non è dato sapere di eventuali comunicazioni via chat o altre piattaforme informatiche di comunicazioni tra più soggetti [IRC, messanger, skype (93), ecc.] ma ove vi fossero state non vi sarebbero stati dubbi sull'applicabilità delle garanzie dell'art. 266 bis c.p.p.
In caso di intercettazione di navigazione sulla rete internet il tema è più complesso e meriterebbe una trattazione a parte. Si rimanda pertanto su quest'ultimo punto a opere più specifiche che hanno affrontato anche tecnicamente la tematica (94).
Le caratteristiche tipiche specifiche del software trojan utilizzato fin dal 2004 non sono note, ma sarebbe utile la loro presenza negli atti del processo a garanzia delle operazioni compiute dal nuovo sistema tecnologico intrusivo. Ciò che emerge dalla sentenza è sufficiente però per capire almeno in parte cosa è stato (ed è..) in grado di fare tale software (95).
Gli apparati investigativi sono stati in grado di inoculare e installare sul PC dell'indagato un programma ''fantasma'' capace di inviare in maniera occulta tutti i documenti in formato word che l'indagato scriveva e tutte le aggiunte o correzioni che con il tempo (8 mesi) eseguiva sui documenti word redatti e memorizzati sull'hard disk del computer d'ufficio dell'indagato (non sembra fosse un PC portatile). Non erano affatto documenti che il soggetto inviava a terzi o che inviava per posta elettronica o pubblicava sulla rete internet e quindi non erano comportamenti comunicativi.
Stupisce anche il punto in cui la Corte di Cassazione ritiene che la prova raggiunta sia una prova atipica e quindi disciplinata dall'art. 189 c.p.p. In realtà, a ben vedere, trattandosi di files informatici contenuti su supporti informatici tipizzati e introdotti nel nostro ordinamento con la legge n. 547/1993, forse qui non è tanto in discussione la prova atipica ma il mezzo con la quale è stata acquisita la prova e quindi l'utilizzo di mezzi atipici di ricerca della prova.
Parte della dottrina (96) si domanda se siano configurabili mezzi di ricerca della prova atipici soprattutto quando le circostanze di fatto e di diritto consentono di acquisire gli elementi di prova attraverso l'utilizzo dei tipici mezzi di ricerca come perquisizioni, sequestri o ritardati sequestri. Si tende a negare tale categoria non prevista dal codice di procedura rilevando che i mezzi di ricerca della prova sono posti in essere prevalentemente nel corso delle indagini pre-

liminari in situazioni nelle quali è impossibile il contraddittorio con la difesa davanti al giudice come indica l'art. 189 c.p.p.
Di contro, le Sezioni Unite della Cassazione (97) hanno affermato che è possibile configurare mezzi di ricerca della prova atipici come per esempio le video-riprese d'immagini in luoghi diversi dal domicilio attraverso un'interpretazione adeguatrice dell'art. 189 c.p.p. nel senso di configurare un contraddittorio posticipato e successivo sull'utilizzabilità degli elementi acquisiti (98). La medesima pronuncia ha anche affermato che ove le video-riprese avvengono invece in luoghi domiciliari o di privata dimora non sono utilizzabili quelle aventi ad oggetto comportamenti non comunicativi. È di tutta evidenza che soltanto un'interpretazione della norma in questo senso è rispettosa del principio di legalità della prova.
Nel caso del trojan usato come captatore informatico è ancora più evidente che una interpretazione in questo senso dell'art. 189 c.p.p. può essere agevolmente condivisa solo e in quanto il personal computer sottoposto ad ''acquisizione'' non è classificabile come domicilio informatico.
La Corte di Cassazione non convince affatto quando sul punto ritiene «che, nella specie, dovesse essere osservata la disciplina prevista per gli accertamenti tecnici irripetibili, atteso che l'attività di riproduzione dei files memorizzati non aveva comportato l'alterazione, né la distruzione dell'archivio informatico, rimasto immutato, quindi consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria. Si era trattato di un'attività sempre reiterabile, alla cui esecuzione non era necessaria la partecipazione del difensore, poiché la stessa avrebbe potuto essere compiuta una seconda volta se si fosse approdato ad uno sviluppo dibattimentale del procedimento».
Con riferimento alla mancata osservanza della disciplina prevista per gli accertamenti tecnici irripetibili (artt. 359 e 360 c.p.p.) e al mancato avviso alle parti e ai difensori la Suprema Corte però non convince perché non ha tenuto conto né ha motivato che:
– un sistema informatico sottoposto ad intrusione da parte di un ''Trojan di Stato'' è comunque alterato a livello strutturale e informatico;
– con il cosiddetto ''captatore'' all'interno del sistema informatico mutano alcune funzioni di sistema specifiche che consentono ad un operatore da remoto e connesso alla rete di prendere il possesso dello strumento e di far compiere allo strumento stesso una serie di operazioni fuori dal controllo dell'utente autorizzato modificando molte funzioni tipiche di sicurezza del sistema;
– di eseguire una serie di funzioni tipiche del software conosciute soltanto dal creatore dello stesso;
– di alterare anche accidentalmente il contenuto del sistema informatico non consentendo alla difesa di ripetere l'operazione di acquisizione;
È assai discutibile sostenere, come fa la Corte, che l'attività è sempre reiterabile in quanto è possibile compierla anche una seconda volta al momento del dibattimento. È come dire che una perquisizione domiciliare (irripetibile per eccellenza) è ripetibile ''*n*'' volte perché la difesa può tornarci quando vuole dopo che il locale è stato perquisito dalle forze di polizia. Non è proprio così o comunque non è assolutamente stato dimostrato come sia stata garantita la genuinità e integrità dei files acquisiti.
Esistono ed esistevano anche nel 2004 sistemi e procedure tecniche in grado di garantire che un file prima e dopo l'acquisizione non veniva modificato e che la copia effettuata può essere poi verificata dalla difesa e valutata nella sua integrità e genuinità (99).
Stiamo parlando delle tecniche di hashing che avrebbero potuto garantire l'integrità e la genuinità dei file captati da remoto se effettuate prima dell'operazione e soprattutto con criterio e con la finalità di dimostrare poi alla difesa la genuinità della prova.
Questo tema è molto importante e delicato perché non può tacersi l'utilità di risolvere, anche legislativamente, il problema giuridico dell'ammissibilità di uno strumento tanto pericoloso quanto utile ed efficace in alcuni contesti specifici (criminalità organizzata, utilizzo illecito di sistemi criptati e di cloud computing allocati in server residenti in remote e sconosciute regioni del mondo, sistemi informatici e dati/informazioni non acquisibili altrimenti, ecc.).
Fermandosi a ciò che è noto attraverso l'analisi dei software in commercio sulla rete, ma consapevoli che nella pratica si tratta di strumenti ben più evoluti, vale la pena elencare qualche specifica tecnica, alcune criticità e le possibili soluzioni con il rispetto delle garanzie processuali.
Un software trojan in dotazione alle forze di polizia in quanto acquistato o noleggiato da società private italiane e straniere, oggi è in grado di:
– entrare nel sistema ''target'' e prende il completo controllo di tutte le funzioni inibendo l'antivirus e controllando anche la webcam, la navigazione e la posta elettronica (sia web mail sia di outlook);
– è in grado di attivare i microfoni del sistema e ascoltare ciò che avviene nelle vicinanze del PC come una vera e propria intercettazione ambientale o comunque è in grado di intercettare eventuali comunicazioni telefoniche o telematiche effettuate con il sistema informatico (alcuni provvedimenti giudiziari, per questa attività, hanno già confermato e ritenuto correttamente necessario il decreto di intercettazione del Giudice per le indagini preliminari);
– è programmato per sfuggire agli antivirus in commercio;

– acquisisce e recapita on line all'investigatore, ad intervalli di tempo predefiniti a piacere e quindi in tempo reale, tutto il contenuto del PC (ogni tipo di file, log di navigazione web, posta elettronica, foto, screnn shots dei siti web visitati);
– si può autodistruggere con un comando appositamente predisposto pulendo le sue tracce all'interno del PC ed è difficilissimo capire ma soprattutto dimostrare successivamente se e quando è stato istallato e soprattutto qual è stata la sua attività;
– può uplodare ovvero inoculare e memorizzare nel sistema informatico ''target'' qualsiasi tipo di file salvandolo a piacimento in qualsiasi parte del sistema;
È chiaro che quest'ultima è un'operazione illecita che mai sarà svolta da una forza di polizia soprattutto se coordinata da una Procura della Repubblica ma possiamo ritenere che tali strumenti siano sempre sotto il controllo dell'Autorità Giudiziaria?
È una tecnica di ''remote forensics'' delegata troppo spesso soltanto a consulenti nominati ausiliari di polizia giudiziaria che operano però lontano da un controllo di quest'ultima e tantomeno da quello del pubblico ministero. Non si ravvisano obblighi di redigere puntuali annotazioni con menzione di tutti i particolari dell'operazione occulta, degli strumenti utilizzati nonché delle date e degli orari delle operazioni svolte.
Tutto ciò è molto più di un'intercettazione telefonica o telematica che, in quanto tale, necessita dell'ausilio dell'operatore telefonico e quindi di un terzo con conseguente tracciamento esterno delle operazioni. Qui non c'è tracciamento delle operazioni di captazione da remoto del contenuto di un computer o di uno smartphone, o meglio, nulla è previsto dalle norme vigenti o dalla prassi.
Vale la pena pertanto di sollevare alcune critiche che vanno ad aggiungersi alle perplessità già espresse in precedenza:
Il trojan altera il computer ''target'' e appare in contrasto con quanto stabilito dalla legge n. 48/2008 e dalle modifiche al codice di procedura penale; sarebbe quindi opportuno, allo stato, utilizzarlo ad esempio solo quando la legge consente il ricorso al ritardato sequestro (reati di associazione a delinquere di stampo mafioso ecc.); il software capta, monitorizza, registra anche comportamenti non comunicativi che non sono utilizzabili se tenuti all'interno di un domicilio (informatico); occorrerebbe pertanto porsi il problema se, nella prassi o de iure condendo, non sia il caso di differenziare l'attività di indagine su sistemi informatici ''privati'' e su quelli ''pubblici''.
Ad avviso di chi scrive è necessario valutare se siamo di fronte ad un mezzo di ricerca atipico giustificato da esigenze reali e non altrimenti risolvibili. In altri termini, verificare se esiste la possibilità concreta di arrivare o meno all'acquisizione del contenuto del PC in altro modo, ad esempio attraverso una perquisizione e un sequestro del computer secondo il metodo classico (oppure, come si diceva sopra con il ritardato sequestro nei casi consentiti dalla legge). Soltanto in caso di assoluta impossibilità ad acquisire il contenuto in queste forme e con questi mezzi tipici di ricerca della prova, come sopra ricordato, si potrebbe giustificare il ricorso a mezzi atipici come il ''captatore informatico''. È questo il caso di sistemi informatici (es. servers, proxy, sistemi Cloud o Intercloud) allocati all'estero, magari in paesi che non forniscono assistenza alle richieste di rogatoria, oppure a dati allocati magari su piattaforme di cloud computing protette da sistemi di cifratura inattaccabili o comunque per loro natura non accessibili se non on line e con l'utilizzo di segretissime e complesse parole chiavi. Ecco magari in tutti questi casi potrebbe spiegarsi meglio (in diritto e in fatto) l'utilizzo del ''virus di Stato'' come mezzo atipico di ricerca della prova.
Un altro punto di criticità all'utilizzo del ''captatore'' è l'assenza di qualsivoglia controllo diretto e ufficiale sull'attività che svolge l'operatore addetto alla captazione di tutto il contenuto del sistema ''target''. Quale garanzia ha il pubblico ministero che ha emesso il decreto e autorizzato la captazione sull'attività svolta nel caso in cui decide di ricorrere ad ausiliari di polizia esperti o a veri e propri consulenti tecnici? Un ufficiale di polizia giudiziaria assiste sempre a tutte le operazioni che vede e fa il tecnico davanti al proprio sistema? Sono tutte domande alle quali non è possibile dare risposta perché la procedura non è disciplinata ed è lasciata alla sensibilità delle diverse squadre di polizia giudiziaria e delle procure.
Ad esempio, ad avviso di chi scrive, la redazione di un verbale di polizia giudiziaria, con il dettaglio delle operazioni eseguite nomina di eventuali ausiliari, l'indicazione delle specifiche tecniche del software (100), l'indicazione di date e orari nonché il dettaglio sintetico del monitoraggio effettuato, risolverebbe alcuni problemi.
Sarebbe altresì auspicabile una contemporanea attività di intercettazione telematica dei flussi informatici del sistema ''attaccante'' (una vera e propria autointercettazione telematica o al limite l'utilizzo di un keylogger con firma digitale applicato al sistema che controlla il trojan) e quindi dell'utenza della polizia giudiziaria o/consulente tecnico al fine di monitorare e garantire l'indagato da upload anche involontari che altererebbero la scena criminis.
Altra forma di garanzia delle operazioni potrebbe essere anche un'attività di logging di tutta l'attività che giornalmente svolge il client (Personal Computer) ''attaccante'' (101), con apposizione di firma digitale e marcatura temporale ai file prodotti dal sistema nonché ai file relativi all'acquisizione.
A ben vedere, concretamente il programma utilizza-

to capta in tempo reale anche gli screen shot (delle vere e proprie foto dello schermo) relativi alla navigazione in internet nonché le comunicazioni via chat (di ogni genere e social network, pertanto non è vero quando affermato in alcune pronunce o da qualche G.I.P. (ad oggi pochi a dire il vero) che è necessario soltanto il decreto per l'eventuale intercettazione "ambientale". Al contrario infatti è necessario considerare anche le su menzionate attività di documentazione dei flussi telematici, ad avviso di chi scrive, soggette alla disciplina dell'art. 266 bis c.p.p. e quindi sottoposte al vaglio del giudice per le indagini preliminari.

Ciò racchiude in sé un altro problema di fondo: in uno stato di diritto con garanzie processuali codificate la corsa al risultato a tutti i costi non può comprimere le garanzie processuali, le garanzie difensive e il dovuto controllo del giudice per le indagini preliminari sugli strumenti investigativi che mettono in pericolo il contenuto delle comunicazioni e la riservatezza del domicilio (anche informatico).

Sarebbe auspicabile che il Legislatore intervenga sulla questione, paradossalmente anche per poter sbloccare quelle situazioni investigative nelle quali veramente il sistema di captazione occulto da remoto è l'unico modo per acquisire il contenuto di servers altrimenti irraggiungibili (102).

La mancata tipizzazione dello strumento di ricerca produce almeno tre distorsioni : scoraggia l'investigatore consapevole, scrupoloso e attento; mette in pericolo la riservatezza di tanti cittadini e non garantisce sull'acquisizione di dati utili alle indagini.

STEFANO ATERNO

(89) Cass. pen., sez. V, 14-10-2009, n. 16556, *CED*, 246954.

(90) Software Trojan nascosto che consente all'utilizzatore di prendere il completo controllo del computer o dello smartphone; all'epoca probabilmente fu utilizzato un Software dal nome "Back Orifice".

(91) Si consenta un rinvio all'unico articolo pubblicato in materia, ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto*, *Memberbook IIsfa*, 2012, Forlì.

(92) Il virus necessariamente inviava attraverso la rete i dati captati alla stazione ricevente degli investigatori.

(93) All'epoca dei fatti di cui in sentenza (2004), il sistema di comunicazione via skype non era ancora stato inventato.

(94) ATERNO-CAJANI-COSTABILE-MATTIUCCI-MAZZARACO, in *Manuale di Computer Forensics*, cit., 2012. Si veda, per una prima analisi tecnica sul punto, MARIOTTI-TACCONI, in *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni voip*, *Dinternet*, 2008, 558 ss.

(95) Oggi questi software sono molto più evoluti rispetto al 2004 e in grado di svolgere attività ancora più sofisticate; si veda, per un utilizzo molto commerciale e ormai comune e diffuso, il software win spy, scaricabile dalla Rete e facilmente rintracciabile digitando il nome nei motori di ricerca.

(96) TONINI, *Manuale di procedura penale*, cit., 258.

(97) Cass. pen., S.U., 28-3-2006, n. 26795.

(98) TONINI, *Manuale di procedura penale*, cit., 258.

(99) Tecniche e procedure di hashing note soprattutto oggi in quanto la legge n. 48/2008 ha introdotto particolari disposizioni che necessitano di tali accortezze ma non vi è dubbio che sono tecniche conosciute a livello informatico anche nel 2004 tra le forze di polizia che effettuavano tali indagini ma delle quali non c'è menzione nella sentenza.

(100) La difesa deve sapere cosa ha fatto o è in grado di fare il software introdotto nel sistema.

(101) Per questo potrebbe essere utilizzato un sistema di keylogger implementato sulla macchina che intercetta/capta e quindi riceve il contenuto del sistema "target" in modo da registrare e garantire ogni attività che svolge il "trojan di stato".

(102) Vedere appunto i casi tipici di illeciti commessi a mezzo di piattaforme di cloud computing o sistemi proxy.