Poliziamoderna

Prova informatica e processo penale

1. Introduzione Da qualche decennio gli strumenti probatori del processo penale si stanno arricchendo, poiché all'usuale e tradizionale catalogo dell'accertamento penale si sono aggiunti elementi di prova scientifici e tecnologici che hanno posto problemi giuridici, che il legislatore, la dottrina e la giurisprudenza hanno tentato di risolvere. Lo spazio processuale che maggiormente risente dei problemi posti dalla prova scientifica è quello riguardante le indagini informatiche, concernano esse i reati comuni commessi occasionalmente con lo strumento informatico, oppure i casi, sempre più numerosi, nei quali le prove dell'illecito possono essere ricavate da dispositivi digitali, oramai posseduti dalla quasi totalità della popolazione. L'asserita fragilità della prova informatica, che può essere facilmente modificata, alterata o danneggiata, volontariamente o per imperizia, solleva il problema, scientifico e quindi giuridico, dell'acquisizione sicura dei dati e della ripetibilità dell'operazione. La legge 18/2/2008 n. 48 ha inquadrato le attività di ricerca della prova informatica fra i mezzi tipici disciplinati dal codice di procedura, ma ha evitato di dettare un protocollo di raccolta della prova, limitandosi, con saggezza, a indicare le esigenze che debbono essere soddisfatte (conservazione dei dati originali, conformità della copia all'originale, assenza di alterazioni). La giurisprudenza della Corte Suprema e la dottrina hanno studiato e risolto alcuni problemi processuali e di tutela dei diritti individuali che la novità della materia aveva fatto sorgere. Si è quindi esaminata la giurisprudenza secondo la quale la raccolta dei dati informatici non costituisce un accertamento tecnico irripetibile soggetto alla disciplina dettata dall'art. 360 cpp. Si sono inoltre illustrate le decisioni che hanno sancito che i provvedimenti che dispongono la ricerca di una prova informatica non devono necessariamente specificare quale sia il materiale rilevante da ricercare, essendo sufficiente che il provvedimento indichi fra le cose da sequestrare quelle che hanno capacità dimostrative rispetto a un supposto reato. Si è accertato, alla luce della corrente giurisprudenza, che i messaggi di posta elettronica devono essere giuridicamente definiti come "corrispondenza" e vanno quindi sottoposti alla normativa che riguarda questa categoria di oggetti. I problemi giuridici riguardanti i mezzi di ricerca della prova sorgono man mano che l'attività istruttoria si dipana, ma essi assumono importanza decisiva nel dibattimento, quando si decide se essi possano concorrere, oppure no, a determinare il contenuto della decisione. Il dibattimento costituisce il luogo topico, non solamente nella astratta teoria del processo, perché solamente in esso si accerta se le attività investigative siano state corrette o meno e siano state, quindi, utili ed efficaci. Si è esaminato, pertanto, sotto quale veste i dati informatici sono acquisiti nel processo e si è accertato, alla luce della legislazione e della giurisprudenza, che essi fanno parte dei "documenti" disciplinati dall'art. 234 cpp. Si sono analizzate le forme e i casi di acquisizione dei medesimi: se su richiesta delle parti e previo esame della sussistenza dei presupposti descritti dagli artt. 493-495 e 190 cpp; oppure per inserzione preliminare nel fascicolo per il dibattimento a norma dell'art. 431 cpp. Si sono poi verificate le eventualità che la parte interessata possa opporsi all'acquisizione dei documenti informatici e si sono descritti la natura, il contenuto e l'iter dell'opposizione. Ci si è soffermati sulle procedure e sul contenuto della valutazione, da parte del giudice, della prova scientifica, che sfugge ai normali e tradizionali canoni dell'applicazione di massime di esperienza e del senso comune ma che deve essere sottoposta a critica alla luce di alcuni criteri precisati dalla dottrina e dalla giurisprudenza, del cui uso il giudice deve dare esauriente conto nella motivazione. Si sono infine esaminate le potenzialità probatorie della prova informatica che, contrariamente alle comuni credenze, normalmente fornisce dati meramente indiziari, che devono essere pertanto confortati dai tradizionali mezzi di indagine.

2. Prova informatica e processo penale 2.1 LA PROVA SCIENTIFICA Il codice di procedura penale del 1988, tuttora vigente, si ispira, come già quello del 1930, al principio del libero convincimento, secondo il quale il giudice valuta in maniera discrezionale, e non secondo il metodo delle prove legali, l'efficacia probante del mezzo istruttorio assunto. La prova, nel processo penale, tende a far conoscere un avvenimento verificatosi nel passato mediante un fatto direttamente constatabile nel presente: essa può essere considerata concludente quando si riveli utile a dimostrare l'esistenza del fatto da accertare mediante l'applicazione delle massime di esperienza, delle comuni regole di giudizio, che sono fallibili e incerte e conducono a più di una soluzione, fra le quali il giudice deve scegliere quella che sembra la più idonea. Il sistema prescelto esige rigorosi parametri di valutazione ai quali il giudice deve necessariamente attenersi e che non può trascurare nel momento in cui deve esaminare le prove. Ad evitare poi che la libertà di valutazione possa tramutarsi in arbitrio, è previsto (art. 111 Cost) che il giudice debba motivare i suoi provvedimenti perché le parti possano rendersi conto delle ragioni della decisione; inoltre l'art. 192 cpp stabilisce che il giudice debba dar conto nella motivazione "dei risultati acquisiti e dei criteri adottati" nella valutazione della prova e la lettera e) del primo comma dell'art. 546 specifica che il giudice deve analizzare tutti i risultati istruttori acquisiti e

deve indicare nella motivazione gli elementi posti a base della decisione e le ragioni per le quali ritiene inattendibili quelli contrari. Deve, cioè, dare conto del metodo adottato per valutare le prove che, tradizionalmente, è, o era, quello basato sul senso comune, sul catalogo delle conoscenze empiriche, sugli strumenti culturali propri dell'appartenente a una certa società, sulle massime d'esperienza, che sono regole di giudizio comunemente riconosciute e accettate. Quel metodo di valutazione delle prove sta entrando in crisi. Da tempo, e sempre più velocemente e massicciamente, i fatti rilevanti del processo penale possono o devono essere dimostrati con teorie e alla luce di leggi scientifiche o con procedure e strumenti tecnici. Gli esempi sono innumerevoli e lampanti e non v'è bisogno di esemplificazioni. L'utilizzazione della prova scientifica nel processo tende a confinare il senso comune in ambiti più ristretti tanto che "lo spostamento della linea di confine tra il sapere comune e il sapere specialistico rischia di sottrarre all'organo giudicante competenze valutative e decisionali che riesce difficile non considerare appartenenti al suo esclusivo dominio".

2.2 LA PROVA DIGITALE Un settore della prova scientifica che ha assunto una sicura rilevanza e si avvia a svolgere un ruolo particolarmente importante nel panorama processuale – non solamente penale – è quello riguardante l'informatica. Rientra nella comune esperienza la continua e sempre più abbondante diffusione e utilizzazione di dispositivi digitali, quali computer, CD, DVD, hard disk, pen drive, chiavette usb, telefoni cellulari, iPod, gps, fotocamere e videocamere digitali, orologi multifunzione, bancomat, telepass (l'elenco è largamente incompleto e viene aggiornato di continuo), che sono apparecchiature capaci di memorizzare e conservare una infinita serie di dati, informazioni, rappresentazioni di fatti che riguardano una parte significativa della vita, dei rapporti, delle attività di lavoro, di svago, lecite o illecite, morali o immorali di un numero già smisurato ma sempre crescente di persone. Il fenomeno è diventato tanto esteso da essere oggetto di ricerche e studi sociologici, comportamentali, educativi, pedagogici e che, appunto per la sua importanza, non poteva non entrare a far parte, sotto varie sfaccettature, del diritto penale. Nel mondo anglosassone – che ha conosciuto un precoce sviluppo dell'uso di quelle apparecchiature – sono nate delle branche del diritto penale sostanziale e processuale che le riguardano: i computer crimes (a esempio quelli introdotti in Italia dalla legge 23/12/1993 n. 547, concernenti attacchi a integrità di banche dati e sistemi informatici) e i computer-related crimes (truffe telematiche, clonazione di documenti, diffamazioni o ingiurie, e tanto altro) nei quali il dispositivo digitale può essere l'obbiettivo di atti criminali o il mezzo per compierli. E ci sono ancora i casi, più numerosi, più interessanti dal punto di vista dei riflessi sulle indagini, nei quali le apparecchiature contengono informazioni, memorizzate o trasmesse in formato digitale (digital evidence), riguardanti un qualunque reato, che possono essere utili ai fini delle indagini e formano oggetto della computer forensics, la "scienza che studia le problematiche tecniche e giuridiche correlate alle investigazioni sui dati digitali" e ha come fine quello di identificare, acquisire, documentare e conservare le informazioni contenute in un computer, assicurando che non avvengano mutamenti del sistema. Quelle apparecchiature costituiscono pertanto fonti di prova, dato che dall'hard disk dell'elaboratore possono essere prelevati e utilizzati dati rilevanti per l'indagine, che costituiscono gli elementi di prova, quali il piano di una rapina, le fotografie di un omicidio, immagini pedopornografiche e tanto altro. Ma si possono eventualmente rinvenire argomenti a favore della difesa, come un alibi desunto, ad esempio, da fotografie, dall'utilizzo del computer in un certo lasso di tempo o da altri elementi che potrebbero escludere che l'indagato sia l'autore del reato. La prova digitale, in definitiva, è qualunque informazione che può assumere la veste di elemento di prova, memorizzata o trasmessa in un formato digitale.

2.3 LA FRAGILITÀ DELLA PROVA INFORMATICA I computer e gli apparecchi digitali sono composti in realtà da due parti distinte. Vi è una parte fisica, e cioè un oggetto materiale che si può vedere e toccare e che va trattato come un qualsiasi altro oggetto che sia ritenuto interessante ai fini delle indagini, poiché può trattenere sulla carcassa o sulla tastiera impronte digitali e altre tracce fisiche anch'esse utili all'indagine. Vi è poi una parte invisibile, logica, contenuta nei supporti di memoria. Tutti i dati di cui si parla sono memorizzati, sotto forma di bit, su memorie di tipo magnetico o magneto-ottico ed elettrico. La memoria, l'unità di immagazzinamento, contiene una lunghissima serie di informazioni e di dati relativi all'utilizzazione e conserva traccia persino di molte operazioni che l'utente ha eseguito nel corso dell'impiego della macchina. I dati, anche se cancellati, salvo sovrascritture non vengono eliminati e possono essere richiamati in vita anche se sia trascorso molto tempo dal momento della soppressione. L'enorme congerie di informazioni, che l'apparecchiatura contiene, rende lungo e difficoltoso il processo di ricerca ed esame dei file che possono essere interessanti da un qualche punto di vista, come può essere quello dell'indagine penale. La particolare natura – immateriale e volatile – dei dati contenuti in un dispositivo tecnologico comporta che essi possano essere modificati, alterati, danneggiati, distrutti anche inavvertitamente, da un'errata operazione specialmente da chi li manipoli senza essere tecnicamente preparato. È importante, quindi, agire con grande cautela e sufficiente perizia tecnica per cercare, esaminare ed estrarre elementi di prova da uno di quegli apparecchi. Il momento più delicato dell'attività della pg riguardo alla prova digitale è costituito dall'acquisizione di essa in maniera tecnicamente idonea, in modo tale da consentire l'inalterabilità della memoria del dispositivo. Ma è anche necessario che il soggetto operante si assicuri che la fonte di prova non abbia subìto contaminazioni, sia dopo che i dati siano stati raccolti, che nel corso della procedura di analisi, per rendere credibili, attendibili e riproducibili i

risultati dell'esame. È palese che i problemi che sorgono riguardo alle investigazioni informatiche concernano, in primo luogo, l'uso delle procedure di carattere tecnico più idonee a raccogliere le informazioni contenute in un computer. Ma è necessario inquadrare tali attività all'interno delle regole relative al sistema delle prove, la cui osservanza deve tendere a garantire che il materiale probatorio possa essere utilizzabile in giudizio. Dal punto di vista tecnico sorge il problema dell'esistenza di una numerosa serie di spesso divergenti protocolli operativi standardizzati, riguardanti la procedura di acquisizione della prova scientifica, che sono in perenne evoluzione in relazione al rapido mutamento delle tecnologie e che fanno diventare sorpassati i mezzi d'intervento. Tali banali osservazioni hanno fatto escludere la possibilità che la legge possa direttamente provvedere a regolamentare le procedure di acquisizione delle prove scientifiche, poiché quelle norme dovrebbero essere continuamente adeguate ai costanti mutamenti della scienza e della tecnologia.

2.4 LE NORME PROCESSUALI Con la legge 18 febbraio 2008 n. 48 lo Stato italiano ha ratificato e dato esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23 novembre 2001, e ha così aggiornato alcune norme del III e del IV libro del codice di procedura penale concernenti le prove e le indagini, consentendo ispezioni, perquisizioni, sequestri e accertamenti urgenti di pg riguardo a sistemi o programmi informatici e telematici, anche se salvaguardati da misure di sicurezza. La nuova normativa non ha regolamentato nel dettaglio le operazioni di acquisizione di notizie informatiche, ma ha indicato pragmaticamente quale debba essere il risultato finale da conseguire piuttosto che il metodo per raggiungerlo, evitando così una scelta fra vari possibili protocolli che, come s'è già detto, sono innumerevoli e soggetti a frequentissimi aggiornamenti in conseguenza dell'evoluzione continua della disciplina. Il legislatore ha invece indicato la necessità di soddisfare alcune esigenze dirette a: consentire la conservazione dei dati originali; impedirne l'alterazione nel corso delle operazioni di ricerca delle fonti di prova; garantire la conformità della copia all'originale, nonché la sua immodificabiltà quando si proceda ad una duplicazione; dotare di sigilli informatici i documenti appresi. Le modifiche apportate dalla legge n. 48 del 2008 hanno riguardato alcuni punti del codice di procedura penale: in tema di ispezioni, all'art. 244 comma 2 secondo periodo sono state aggiunte le parole: "anche in relazione a sistemi informatici, telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione"; all'art. 247, che concerne casi e forme delle perquisizioni, è stato inserito il comma 1 bis: " Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché non protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione"; è stato sostituito il primo comma dell'art. 254, riguardante il sequestro di corrispondenza, col seguente: "Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere 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"; è stato aggiunto l'art. 254 bis : "Sequestro di dati informatici presso fornitori di servizi informatici, telematici o di telecomunicazioni. – 1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei servizi medesimi, che la loro acquisizione avvenga mediante la copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali"; nel primo comma dell'art. 256, che riguarda il dovere delle persone indicate dagli artt. 200 e 201 di consegnare immediatamente atti e documenti, sono state aggiunte le parole: "nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto"; al secondo comma dell'art. 259, riguardante gli obblighi del custode delle cose sequestrate, è stato aggiunto il periodo: "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"; l'art. 260 prevede ora che il sigillo alle cose sequestrate possa essere apposto con mezzi "anche di carattere elettronico o informatico"; nell'art. 352, che riguarda le perquisizioni a iniziativa della polizia giudiziaria, è stato inserito il comma 1 bis: "Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi"; l'art. 353 prevede che il pm autorizzi la pg a ricercare notizie utili all'assicurazione delle fonti di prova non solamente con l'immediata apertura di plichi, ma anche con l'"accertamento del contenuto" della corrispondenza informatica; dopo il primo periodo dell'art. 354 ("accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro") è stato aggiunto: "In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informativi o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurare la conservazione e a 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". Le garanzie indicate dalla novella del 2008 hanno l'evidente finalità di assicurare l'acquisizione di elementi di prova genuini e attendibili e di raggiungere l'obbiettivo di salvaguardare, a tutela dei diritti della difesa, la possibilità del controllo successivo dell'attività degli inquirenti, che deve concernere in primo luogo la verifica del metodo utilizzato per l'acquisizione. I procedimenti scientifici riguardanti l'informatica e la raccolta della prova digitale, come detto, sono in continua evoluzione. È sorto in passato il dubbio che, in relazione alla novità che le riguardano, l'assunzione di quelle emergenze probatorie dovesse ritenersi regolata dall'art. 189 cpp, cioè dalla norma nata sia per disciplinare situazioni contrassegnate da caratteristiche di novità, che per evitare eccessive limitazioni all'accertamento della verità in relazione al "continuo sviluppo tecnologico che estende le frontiere dell'investigazione", richiamato dalla Relazione al progetto preliminare del cpp. L'applicazione della disciplina dettata dal citato art. 189 implica che il richiedente dimostri l'idoneità della prova atipica ad accertare i fatti, anche in relazione alla "affidabilità dei metodi e delle procedure adottate dall'esperto". È sorto però il dubbio che quella norma potesse riguardare esclusivamente gli strumenti scientifici nuovi o controversi (accertamento che lascerebbe uno spazio eccessivo alla discrezionalità in relazione alla definizione dei detti requisiti), sia perché essa non contiene un'indicazione specifica in tal senso, sia perché quella regolamentazione potrebbe essere applicabile anche ad altri collaudati mezzi di prova scientifica il cui svolgimento non sia però regolato dalla legge. La novella del 2008 ha ricondotto le attività di ricerca e raccolta della prova informatica nel novero dei mezzi tipici disciplinati dal codice con la conseguenza che anche riguardo all'ammissione delle prove informatiche si applicano le regole dettate dall'art. 190 cpp. Da ciò consegue che una prova che sia fondata su teorie o procedimenti scientifici inaffidabili non può essere ammessa poiché "la prova non autenticamente scientifica è manifestamente irrilevante". Nel momento dell'assunzione il giudice deve valutare criticamente l'affidabilità delle procedure e dei metodi scientifici adottati dagli inquirenti sulla base di alcuni criteri fondamentali che sono generalmente indicati nella "accettazione generale da parte degli studiosi… dal grado di controllabilità e falsificabilità del metodo scientifico, l'esistenza di una revisione critica da parte degli esperti del settore, l'indicazione del margine di errore conosciuto…". Naturalmente, vertendosi in tema di prova, è necessario che chi intenda contraddire un elemento istruttorio offerto dalla parte avversa si debba addossare l'onere di indicare gli elementi sui quali si basa l'eccezione. La difesa che contesti gli elementi di prova informatica portati dal pm deve specificare i dati di fatto in cui si sostanzi la violazione e deve fornire gli elementi di giudizio che la facciano ritenere sussistente. È necessario quindi che la parte interessata segnali, e alleghi, protocolli, linee guida, regole tecniche comunemente accettate dagli ambienti scientifici che ritiene siano stati violati nel corso della raccolta della prova e abbiano determinato una qualche distorsione del dato informatico.

2.5 LA RICERCA DELLA PROVA I mezzi di ricerca della prova (ispezioni, perquisizioni, sequestri, intercettazioni) hanno lo scopo di acquisire cose, tracce o dichiarazioni che abbiano attitudine probatoria e, cioè, elementi di fatto preesistenti al compimento del mezzo d'indagine. L'ispezione ha finalità di carattere descrittivo derivante dall'osservazione di persone, luoghi o cose allo scopo di accertare le tracce e gli altri effetti materiali del reato. Essa si esaurisce nella descrizione della realtà. La perquisizione ha una finalità ulteriore, che è quella della ricerca del corpo del reato e delle cose a esso pertinenti che, se necessario od opportuno, sono sottoposti a sequestro e sono poi destinati a far parte del fascicolo per il dibattimento (art. 431 comma 1 lettera h) cpp). I citati mezzi di ricerca della prova riguardano anche i dati informatici a seguito delle integrazioni apportate al codice di procedura penale dalla legge 18/3/2008 n. 48, la quale ha previsto che in tali casi debbano essere adottate misure tecniche idonee ad assicurare la conservazione dei dati originali e a impedirne l'alterazione. La scelta legislativa presuppone la natura fragile e facilmente modificabile del dato digitale, che può essere pregiudicato da attività poco accorte o addirittura involontarie, e rispetto a tale alterabilità prescrive l'adozione di procedure idonee a garantire l'integrità e la genuinità della prova. Le attività di indagine riguardanti la specifica materia assumono una successione particolare in relazione alla circostanza che ciò che si vuole rintracciare è un dato immateriale contenuto in un'apparecchiatura "corporea", rispetto alla quale il documento digitale è autonomo. La ricordata peculiarità comporta che le fasi dell'esame abbiano una particolare articolazione, poiché appare necessario per prima cosa cercare e rinvenire il computer con una perquisizione, quindi procedere al sequestro dell'apparecchio per poi mettere in atto la perquisizione dell'hard disk e infine attuare l'acquisizione dei file rilevanti per l'indagine. Si sostiene che quando il computer costituisce solamente il serbatoio delle prove di un reato non sarebbe necessario procedere al sequestro dello stesso, considerato che la raccolta dei dati potrebbe costituire oggetto di una semplice attività ispettiva eseguita a norma dell'art. 246 cpp. Questa scelta investigativa presenterebbe però, a giudizio della dottrina, un aspetto negativo nel caso in cui dovesse essere rinvenuto un grande volume di elementi contenuti nella memoria, considerato il notevole lasso di tempo occorrente per analizzarli. Un problema ulteriore sarebbe rappresentato dall'impossibilità di eseguire sul supporto originale eventuali analisi di controllo da parte dell'indagato o delle altre parti interessate. L'ispezione dovrebbe essere considerata un accertamento tecnico irripetibile cui sarebbe applicabile la disciplina dettata dall'art. 360 cpp e, di conseguenza, dovrebbe poi entrare a far parte direttamente del fascicolo previsto dall'art. 431 cpp con la connessa piena utilizzabilità in dibattimento. La suddetta caratteristica e il conseguente regime normativo implicherebbero che se si procedesse solamente sulla base del dettato dell'art. 244 cpp, e perciò

senza dare gli avvisi indicati dal citato art. 360, si verificherebbe una nullità d'ordine generale prevista dall'art. 178 cpp. La tesi è giudicata erronea dalla giurisprudenza di legittimità e dalla dottrina. La Corte di Cassazione sostiene, in linea generale, che l'accertamento tecnico presidiato dalla disciplina dell'art. 360 cpp consiste in un'attività di studio e di valutazione critica dei dati pertinenti al reato che viene condotta secondo canoni tecnico-scientifici. Per quanto attiene, invece, ai semplici rilievi, la Suprema Corte sostiene che non si possa applicare il regime di maggior garanzia, anche se essi siano approfonditi e in ipotesi irripetibili, come ad esempio "avviene in tema di prelievo di polvere da sparo finalizzata al successivo esame di stub". Per quanto attiene specificamente alle operazioni di prelievo di dati informatici, la Corte di legittimità ritiene che "non dà luogo ad accertamento tecnico irripetibile la lettura dell'hard disk di un computer… e che 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". Con maggiore aderenza al dettato generale, la Corte suprema ritiene che sia "da escludere che l'attività di estrazione di copia di file da un computer costituisca un atto irripetibile… atteso che 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 la riproducibilità di informazioni identiche a quelle contenute nell'originale". Allargando il raggio dell'osservazione la Corte ha affermato "non dà luogo ad accertamento tecnico irripetibile l'estrazione dei dati archiviati in un computer, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte". La Cassazione ha poi categoricamente escluso che possa essere adottato il regime degli accertamenti tecnici irripetibili nell'attività di riproduzione dei file memorizzati in un computer, dato che essa non comporta "né l'alterazione né la distruzione dell'archivio informatico, rimasto immutato, quindi consultabile ed accessibile nelle medesime condizioni anche dopo l'intervento della polizia giudiziaria". Infine, la giurisprudenza di legittimità ha sostenuto che costituisce "dato di comune esperienza che la stampa di un qualsiasi documento redatto su supporto informatico è operazione meramente meccanica riproducibile teoricamente all'infinito".

2.6 MEZZI DI RICERCA DELLA PROVA E DIRITTI SOGGETTIVI Nel corso delle indagini informatiche il sequestro precede la perquisizione della memoria del dispositivo e la prassi – che favorisce sia la celere restituzione del computer all'avente diritto, sia la ripetibilità dell'acquisizione – suggerisce di creare una copia clone (bitstream image) della memoria che, se ha il vantaggio di evitare alterazioni e modificazioni del contenuto di essa, mette a disposizione di chi investiga una "quantità immensa di dati in gran parte non pertinenti all'accertamento dei fatti oggetto di prova e dai quali si possono ricavare informazioni che… contribuiscono a ricostruire profili importanti della vita privata del soggetto". Si sostiene anche che quando si clona l'intera memoria del computer allo scopo di perquisirla, verrebbe meno la linea di demarcazione fra l'attività di ricerca di uno specifico mezzo di prova e l'attività di ricerca di nuove notizie di reato, e ciò renderebbe illegittima quella parte dell'attività investigativa non giustificata da una particolare ipotesi criminosa. Si dice che l'indicato modo di procedere potrebbe importare la trasformazione della perquisizione e del sequestro da mezzi di ricerca della prova riguardante una precisa notitia criminis, a strumenti di indagini esplorative circa l'esistenza di altri, nuovi reati. Si è pensato di eliminare l'indicato inconveniente ed il connesso attentato ai diritti della persona, sostenendo che "il provvedimento di sequestro informatico dovrà avere, rispetto a un sequestro tradizionale, una motivazione più articolata e dettagliata in punto di modalità di selezione dei dati, non potendosi più accettare… provvedimenti genericamente finalizzati all'esplorazione di tutti i dati digitali contenuti all'interno dell'hard disk, attraverso l'apertura (e quindi la lettura) di tutti i file in esso contenuti, con riserva di selezionare soltanto alla fine quelli utili alle indagini". E si è suggerito che "la selezione del materiale rilevante può e deve essere fatta ex ante attraverso l'indicazione delle domande (parole chiave e altro) da porre all'elaboratore elettronico…". Il suggerimento, dettato da una sana preoccupazione, non pare realizzabile e non viene accettato dalla prassi e dalla giurisprudenza forse perché la particolarità del tema della prova digitale non può far venire meno l'invito ad affrontare i problemi della prova scientifica nel processo penale con un "robusto pragmatismo". Ciò tanto più perché è evidente che se "nell'immaginario collettivo è diffusa l'opinione che gli investigatori informatici siano in grado di estrapolare da un elaboratore o da un supporto di memorizzazione di massa (per es. hard disk o dispositivi usb) qualunque tipo di informazione, anche se la stessa è stata abilmente occultata dall'indagato" bisogna constatare invece che "purtroppo… la verità è completamente diversa" perché gli investigatori debbono "far fronte quotidianamente a una molteplicità di fattori ostativi di natura tecnica, fisica e umana" nel cui elenco – oltre che la cifratura non decrittabile, la sovrascrittura che rende illeggibile il file, il danneggiamento dell' hard disk esposto a campi magnetici – vi sono anche le misure che l'utilizzatore del computer può porre in essere per rendere un qualche dato non visibile agli investigatori con una delle tecniche di anti-forensics. Le indicate difficoltà nel reperimento e nella selezione del materiale informatico devono far confinare nei limiti di una pura aspirazione teorica la pretesa di andare alla ricerca selettiva di qualcosa di cui si sa poco e che appare di difficile o impossibile rinvenimento. Ricorrono comunque, quanto alla perquisizione ed al sequestro informatici, esigenze contrastanti che vanno bilanciate: da una parte l'interesse pubblico all'apprensione di elementi di prova utili alla prosecuzione di un'indagine e alla successiva decisione di merito; dall'altra, l'interesse alla tutela dei diritti e delle garanzie processuali dell'indagato o del terzo che subisce materialmente il sequestro.

2.7 I PRINCIPI DELLA GIURISPRUDENZA È opportuno e necessario, a questo punto, verificare puntualmente quali siano i "principi ripetutamente affermati" dalla giurisprudenza di legittimità riguardo ai presupposti che devono ricorrere per dar corso all'adozione dei mezzi di ricerca della prova. Una recente sentenza della Corte di Cassazione ha analiticamente ripercorso l'orientamento dello stesso organo sulla materia, e ha quindi rammentato che: "a) il sequestro probatorio è una misura di ricerca della prova; b) ai fini della legittimità del decreto di perquisizione e del conseguente sequestro, il fumus necessario per la ricerca della prova è quello inerente all'avvenuta commissione dei reati, nella loro materiale accezione, e non già alla colpevolezza del singolo, sicché il mezzo è ritualmente disposto anche qualora il fatto non sia materialmente accertato, ma ne sia ragionevolmente presumibile o probabile la commissione…; c) il sequestro probatorio, proprio perché mezzo di ricerca della prova dei fatti costituenti reato, non può per ciò stesso essere fondato sulla prova del carattere di pertinenza ovvero di corpo di reato delle cose oggetto del vincolo, ma solo sul fumus di esse con il reato". Si deduce dalla chiara lettera della sentenza ora citata che i provvedimenti diretti a ricercare le prove non devono necessariamente indicare con precisione quali debbano essere le cose da ricercare e sequestrare, poiché esse possono non essere determinabili a priori ma devono avere solamente la caratteristica di poter avere attinenza meramente eventuale (fumus) col reato che si presume essere stato commesso. Da tali presupposti consegue che solamente l'esame diretto, illimitato e completo di tutte le cose da ricercare può far scoprire quale di esse costituisca corpo del reato o rivesta la caratteristica di cosa pertinente al reato e debba quindi essere sottoposta al vincolo del sequestro. In applicazione dell'accennato principio di diritto, la stessa Corte di Cassazione, nell'esaminare un "decreto di perquisizione e sequestro di documentazione varia emesso dal pm", ha ritenuto corretto il sequestro di un computer non indicato nel provvedimento perché "nella nozione di documentazione rientra anche quella informatica contenuta nel computer, con la conseguente legittimità del sequestro di quest'ultimo". Il tenore della decisione rende evidente che il provvedimento che dispone la perquisizione e il sequestro di documentazione, anche informatica e riguardante l'intera memoria di un elaboratore elettronico, non deve avere una forma di motivazione particolarmente articolata e dettagliata per la selezione dei dati contenuti nella memoria, ma deve limitarsi a indicare che gli oggetti da sequestrare, "anche senza essere in rapporto qualificato con il fatto illecito, presentino capacità dimostrativa dello stesso". Due recenti sentenze della Corte Suprema hanno fatto il punto sullo stato della giurisprudenza di legittimità riguardo alla questione attualmente all'esame affermando che "non è possibile pretendere l'indicazione dettagliata delle cose da ricercare e sottoporre a sequestro, sia perché il più delle volte le stesse non possono essere specificate a priori, sia perché l'art. 248 cpp, nel prevedere la richiesta di consegna quando attraverso la perquisizione si cerca una cosa determinata, implica che oggetto di ricerca possano essere anche cose non determinate, che potranno essere individuate solo all'esito dell'eseguita perquisizione". La Corte ha poi ulteriormente specificato e spiegato che "nel caso di ricerca di cose non determinate, secondo l'orientamento consolidato di questa Corte, ai fini della legittimità del sequestro di cose ritenute corpo di reato o pertinenti al reato, effettuato dalla polizia giudiziaria all'esito di perquisizione disposta dal pubblico ministero, non è richiesto che le cose anzidette siano preventivamente individuate". Nel completare la disamina delle eventualità che possono presentarsi nelle ipotesi descritte, la Corte ha affermato che "quando invece la pg abbia individuato e sequestrato cose non indicate nel decreto o il cui ordine di sequestro non sia desumibile dalle nozioni di corpo di reato o di cose pertinenti al reato, in relazione ai fatti per i quali si procede, l'Autorità giudiziaria dovrà procedere alla convalida del sequestro ovvero ordinare la restituzione delle cose non ritenute suscettibili di sequestro". E a questo proposito la chiara ed esauriente sentenza concorda con l'orientamento precedente, secondo il quale "in tema di sequestro, qualora il pm, delegando la polizia giudiziaria alla esecuzione di una perquisizione, abbia disposto il sequestro, oltre che degli oggetti e/o documenti esplicitamente indicati, anche di "quanto rinvenuto e in ogni caso ritenuto utile ai fini di indagine", egli è tenuto a provvedere alla convalida relativamente al sequestro avente ad oggetto cose non specificate nel provvedimento". Dalla lettura dell'articolata sentenza della Corte Suprema cui ora s'è fatto riferimento, si deduce chiaramente che il provvedimento di perquisizione e sequestro non deve necessariamente descrivere, e neppure indicare, le cose da ricercare e sequestrare, ma che anzi il pm può delegare alla polizia giudiziaria il compito di sequestrare ogni cosa che, a provvisorio giudizio che quest'ultima può formulare solamente dopo aver analiticamente esaminato tutto ciò che ha rinvenuto, sia ritenuta utile per la continuazione delle indagini. Già in precedenza la Corte di Cassazione aveva affermato la legittimità di un provvedimento che si era limitato a "disporre genericamente il sequestro delle cose rinvenute senza previamente individuarle oppure a formulare in maniera indeterminata l'oggetto della perquisizione (ad esempio indicando genericamente il fine di rinvenire cose pertinenti al reato)" precisando che in casi siffatti l'individuazione delle cose da sequestrare viene affidata alla pg procedente, con la conseguenza che il sequestro deve essere considerato come eseguito direttamente da quest'ultima e deve, di conseguenza, essere oggetto di convalida. Anche la lettura di quest'ultima decisione (che riguarda la perquisizione di un computer) conferma l'orientamento consolidato della giurisprudenza di legittimità, secondo cui il provvedimento di perquisizione e sequestro può avere un contenuto generico e la individuazione di ciò che deve essere sottoposto a vincolo deve essere eseguita dalla polizia giudiziaria, che, va notato, può giungere a scoprire e riconoscere ciò che deve essere sequestrato solamente dopo aver esaminato tutte le cose rinvenute. Cose che, nel caso di perquisizione di un computer, sono tutti i file contenuti nella memoria. Si conferma, così, che risulta non condivisibile l'indirizzo dottrinale secondo il quale i provvedimenti di perquisizione e sequestro del contenuto di una apparecchiatura digitale debbano individuare preliminarmente i file da esaminare. A conclusione

dell'esame dei presupposti per l'emanazione di provvedimenti di perquisizione e sequestro si deve ricordare la giurisprudenza della Corte Suprema secondo la quale l'eventuale illegittimità della perquisizione non produce effetti preclusivi sul sequestro effettuato, qualora vengano acquisite cose che costituiscano corpo del reato o pertinenti al reato, dato che il potere di sequestro, "in quanto riferito a cose obbiettivamente sequestrabili, non dipende dalla modalità con cui queste siano state reperite, ma è condizionato unicamente all'acquisibilità del bene e all'insussistenza di divieti probatori enucleabili dal sistema". Lo stesso principio si ritiene debba regolare il caso del sequestro di computer – nel caso di specie eseguito in relazione al reato di cui all'art. 600 quater cp, anche se in esito a una perquisizione domiciliare autorizzata ai sensi dell'art. 14 della legge n. 269 del 1998 e riguardante il reato previsto dall'art. 600 ter cp – che deve essere giudicato legittimo, poiché si tratta di un atto dovuto eseguito dalla polizia giudiziaria nell'ambito dei poteri conferitile dall'art. 354 cpp.

2.8 I MESSAGGI DI POSTA ELETTRONICA Le preoccupazioni che la dottrina manifesta aumentano quando, procedendo alla perquisizione e al sequestro di elaboratori elettronici ci si imbatte in messaggi di posta elettronica, poiché si sostiene che essi non siano documenti informatici comuni, considerato che la libertà e la segretezza della corrispondenza formano oggetto della speciale tutela apprestata dall'art. 15 della Costituzione e del particolare regime che il codice di procedura penale ha previsto per procedere al sequestro (artt. 254 e 353 cpp). Con la modifica apportata all'art. 254 cpp dalla legge n. 48 del 2008 il legislatore ha posto fine ai dubbi che concernevano l'inquadramento della posta elettronica nel concetto di corrispondenza poiché ha previsto espressamente che si possa intervenire presso i gestori di servizi telematici o di telecomunicazioni per effettuare il sequestro probatorio delle missive inoltrate per via telematica. Le novellate disposizioni degli artt. 254 e 353 cpp introducono alcune deroghe al principio costituzionale della segretezza e dell'inviolabilità della corrispondenza e di qualunque altra forma di comunicazione, pur prevedendo comunque l'adozione di alcune cautele allo scopo di circoscrivere entro limiti ben definiti le compressioni delle garanzie costituzionali. A quello scopo è stato previsto dall'art. 254 cpp che quando all'attuazione del sequestro di corrispondenza provveda (invece che direttamente l'Autorità giudiziaria, come prescrive l'art. 253 co. 3 cpp) un ufficiale di polizia giudiziaria, questi debba consegnare gli oggetti di corrispondenza all'autorità delegante senza aprirli ma anche senza alterarli e senza prenderne altrimenti conoscenza. È significativo il riferimento che la norma citata fa al divieto di "alterare" la corrispondenza, poiché esso riguarda espressamente quella informatica e costituisce un tacito rinvio alle forme della sua acquisizione, che ne garantiscano la conservazione e la immodificabilità. La polizia giudiziaria, invece, non può procedere di propria iniziativa al sequestro di corrispondenza ma, in caso di urgenza e quando ritenga necessaria l'apprensione di plichi che probabilmente contengono notizie utili alle indagini, ordina al preposto all'ufficio postale, telematico o di telecomunicazioni, di sospenderne l'inoltro per il tempo massimo di 48 ore, entro le quali il pubblico ministero può disporre il sequestro (art. 353 comma 3 cpp). Quando invece ricorra un caso d'urgenza la pg può chiedere l'esame immediato e il pm può autorizzare l'apertura della corrispondenza tradizionale e "l'accertamento del contenuto" di quella elettronica, per assicurare fonti di prova che il ritardo potrebbe pregiudicare. Le comunicazioni inviate in forma digitale a un soggetto possono essere archiviate nel computer o nel sistema facente capo a un fornitore di servizi telematici (service provider). I messaggi di posta contenuti in quel sistema possono essere stati già letti dall'interessato, oppure no. La dottrina sostiene la tesi secondo la quale l'acquisizione di messaggi in uscita debba esser fatta alla luce della disciplina dettata dagli artt. 254 e 353 cpp, e che quando si rinvengano "messaggi aperti e nuovi… la posizione più garantista ritiene applicabile ai messaggi non letti la procedura dettata dall'art. 254 cpp con conseguente acquisizione garantita contro alterazioni e trasmissione al P.M. il quale successivamente ne valuterà la sequestrabilità. Di contro per i messaggi aperti la garanzia sopra ricordata non sembrerebbe applicabile in quanto non integrerebbe l'ipotesi di corrispondenza chiusa o sigillata". Due recenti sentenze della Corte di Cassazione hanno delineato sinteticamente il regime delle "intrusioni investigative sulla corrispondenza" chiarendo quale sia lo stato del "diritto vivente" sulla materia. La Corte ha innanzitutto delineato il concetto giuridico di corrispondenza affermando che tale nozione implica "un'attività di spedizione in corso o alla quale il mittente abbia dato comunque impulso consegnandola ad altri per il recapito". Alla luce di questa definizione la Suprema Corte ha affermato che l'art. 254 cpp si pone come disciplina speciale rispetto alla normativa generale dettata dall'art. 253 cpp e concerne solamente "il sequestro della corrispondenza presso uffici postali (o, deve ritenersi, anche in luoghi accessori quali le cassette postali o in via di recapito tramite il portalettere)" e cioè di quella che è ancora in corso di spedizione; mentre ha specificato che "nessuna ragione speciale di tutela – salve le peculiari esigenze attinenti ai rapporti tra imputato e difensore (art. 103 cpp) e le limitazioni imposte alla Polizia giudiziaria nell'acquisizione dei plichi sigillati o altrimenti chiusi, distinti dalla corrispondenza (art. 353 co. 1 cpp – interferisce con l'adozione di un provvedimento di sequestro da eseguire in qualsiasi luogo ove si trovino lettere o pieghi destinati alla corrispondenza o già recapitati al destinatario in base alla generale regola di cui all'art. 253 cpp, in quanto simili cose non sono, appunto, "corrispondenza", implicando tale nozione un'attività di spedizione in corso". Le pronunce di legittimità che si commentano hanno interessato casi aventi a oggetto la corrispondenza ordinaria, ma esse devono essere ritenute applicabili anche a quella elettronica, stante l'equiparazione delle due forme sancita dalle modifiche apportate dalla legge n. 48 del 2008 all'art 254 cpp. Da ciò consegue che le comunicazioni contenute nella memoria di un computer sequestrato oppure in quella di un programma di gestione della posta elettronica, siano esse in partenza perché non ancora

spedite o siano giunte al destinatario, siano state aperte o meno, devono essere considerate oggetto del sequestro ordinario disciplinato dall'art, 253 cpp, dato che quelle missive non possono esser inquadrate nella nozione giuridica di corrispondenza, che secondo la Cassazione ricorre solamente riguardo a quegli oggetti per i quali vi sia "un'attività di spedizione in corso".

2.9 LA PROVA INFORMATICA NEL DIBATTIMENTO 2.9.1 LA PROVA INFORMATICA COME DOCUMENTO Esaminati i problemi che sorgono per la prova informatica nel corso delle indagini, pare opportuno accertare come essa possa concorrere, nel dibattimento, a dar corpo alla decisione. Si è sostenuto che i dati contenuti nel computer sono unici perché la prova che essi forniscono non è "qualcosa di tangibile… (e) presenta caratteristiche che non consentono di assimilarla al documento tradizionale" che è contraddistinto dalla corporalità, mentre la prova digitale si diversifica per la sua "strutturale e intrinseca immaterialità". La diversità fra i due tipi di documenti, ontologicamente esatta circa le caratteristiche che differenziano un documento tradizionale dalla digital evidence, deve essere vista con spirito disincantato e pragmatico, che induce a dover incasellare quella prova in una delle classiche categorie dogmatiche previste dal diritto processuale. Con lo stesso spirito l'ordinamento ha definito con laconica incisività la digital evidence: è un documento informatico, e cioè "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" (art. 1 lettera p) del decreto legislativo 7 marzo 2005 n. 82 - Codice dell'amministrazione digitale). Esso quindi entra nel processo come uno degli "altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo", secondo quanto afferma, con formula che non si presta a equivoci, il primo comma dell'art. 234 cpp. E quindi vanno classificate come "documento" tutte le rappresentazioni di conoscenza, fatti, persone o cose comunque incorporate in qualsiasi base materiale, poiché la reale differenza fra un documento tradizionale e uno informatico è minima, considerato che essa risiede solamente nelle modalità di incorporazione ma non in quelle di rappresentazione, come è stato affermato dalla dottrina, essendo indubitabile che ciò che riveste interesse è il contenuto e non il contenitore. E il concetto era già presente in una risalente sentenza della Corte Costituzionale la quale aveva sostenuto che la definizione data dall'art. 234 cpp identifica il documento in ragione della sua attitudine a rappresentare, essendo irrilevante la differenza "tra i diversi mezzi di rappresentazione e le differenti realtà rappresentate". Anche la giurisprudenza di legittimità ha accolto la teoria ora riferita quando ha affermato con plastica semplicità che "i dati contenuti nel computer costituiscono prova documentale ai sensi dell'art. 234 comma 2 cpp, trattandosi della rappresentazione di cose, termine cui deve attribuirsi la più ampia estensione, effettuata mediante mezzi diversi da quelli tradizionali, così come previsto dalla norma".

2.9.2 LE FORME DELL'ACQUISIZIONE La prova informatica entra, dunque, nel processo come documento. Le vie per l'acquisizione in dibattimento sono, però, diversificate. L'art. 248 cpp prevede che, quando cerca una cosa determinata, l'Autorità giudiziaria possa invitare l'interessato a provvedere alla consegna e che se la richiesta venga accolta possa evitare di procedere a perquisizione. Secondo la dottrina sarebbe necessario incentivare l'uso della richiesta di consegna, onde evitare che la parte veda lesa la propria riservatezza, "mentre l'autorità inquirente sarebbe giustificata a procedere a un atto invasivo solo quando si vedesse opporre un rifiuto o avesse seri motivi per dubitare del comportamento di chi subisce la perquisizione". Similmente il successivo art. 256 dispone che le persone indicate dagli artt. 200 (coloro che sono tenuti al segreto professionale) e 201 cpp (coloro che sono tenuti al segreto d'ufficio) debbano consegnare immediatamente all'A.G. richiedente atti, documenti e dati, informazioni e programmi informatici, anche in copia su adeguato supporto; e prevede che anche in questo la consegna possa rendere inutile il sequestro. Sia nei casi di mancata consegna di quanto richiesto a norma degli artt. 248 e 256 cpp, sia nei numerosi altri casi in cui quella procedura non venga osservata, si procede al sequestro della memoria del dispositivo informatico e alla sua ispezione per la ricerca dei dati interessanti per l'indagine, eseguendo preliminarmente una copia-clone della memoria. Ma è anche previsto che l'acquisizione della copia avvenga all'esito di una perquisizione non seguita da successivo sequestro. La procedura più accreditata, perché ritenuta tecnicamente più idonea e sicura, è quella della clonazione della memoria, mediante la quale si realizza una copia identica al disco rigido originale, certificandone la perfetta corrispondenza a questo, con l'impressione di un algoritmo (codice Hash). Da questa bitstream image si estrae un ulteriore duplicato sul quale si svolgono le indagini. Nel caso in cui queste conducano al rinvenimento di un dato rilevante, questo diventa l'oggetto di un'ulteriore copia particolare. Come entrano nel processo quelle copie, quei documenti? I documenti consegnati ai sensi degli artt. 248 e 256 cpp vengono acquisiti in dibattimento secondo le modalità previste dagli artt. 493, 495 in relazione all'art. 190 cpp: richiesta di parte e conseguente acquisizione ordinata dal giudice quando non siano superflui o irrilevanti né rientrino nella categoria delle prove vietate dalla legge. Quanto ai documenti informatici acquisiti con la modalità del sequestro, essi fanno parte di due categorie. Alla prima appartiene il documento-corpo del reato, come ad esempio quello a mezzo del quale il reato è stato commesso (diffamazione on line, estorsione telematica, pedopornografia in Rete, ecc.). Il secondo gruppo comprende quei documenti che sono utili per l'accertamento di un crimine, e rientrano nell'elenco delle cose pertinenti al reato. I primi, a causa della loro qualità, devono essere inseriti nel fascicolo per il dibattimento in via preliminare ai sensi dell'art. 431 comma 3 lettera h) cpp; gli altri, invece, pur essendo cose pertinenti al reato, devono essere acquisiti con la procedura delineata dagli

artt. 190, 493, 495 cpp alla luce dell'indirizzo secondo il quale i documenti probatori non possono essere inseriti in via preliminare nel fascicolo per il dibattimento ma, appunto, col citato iter che garantisce il contraddittorio anticipato sulla prova. La stessa Corte Costituzionale ha convalidato questa tesi confermando che il verbale di protesto dell'assegno bancario, che riproduce anche la richiesta di pagamento del pubblico ufficiale e la risposta del trattario sull'insussistenza dei fondi, non può entrare nel processo a norma dell'art, 431 cpp ma, essendo prova documentale, deve essere ammessa ai sensi dell'art. 190. Il verbale di sequestro di un computer, dell'hard disk o del documento informatico invece, essendo un atto irripetibile, deve essere inserito per questo motivo nel fascicolo per il dibattimento a norma dell'art. 431 cpp ed è utilizzabile come prova in tutta la sua estensione. Dispone l'art. 511 cpp che deve essere data lettura "degli atti contenuti nel fascicolo per il dibattimento". Secondo una tesi ampiamente accreditata la lettura ha lo scopo di attribuire efficacia probatoria agli atti del fascicolo compiuti nel corso delle indagini preliminari, che in tal modo vengono legittimamente acquisiti e diventano utilizzabili dal giudice a fini di prova. La Corte di Cassazione afferma che la lettura dei documenti ai fini dell'acquisizione probatoria deve ritenersi prescritta per i soli atti contenuti fin dall'inizio nel fascicolo per il dibattimento, mentre non riguarda quelli acquisiti durante l'istruzione dibattimentale. La Corte Costituzionale sostiene invece che, rappresentando il fascicolo dibattimentale un'entità dinamica suscettibile di arricchimenti progressivi, si deve dare lettura di tutti gli atti in esso contenuti, compresi quelli inseriti posteriormente alla sua formazione. Devono essere letti a norma dell'art. 511 cpp anche i verbali di sequestro, per i quali non sussiste il divieto sancito dall'art. 514 comma 2 cpp, che fa salvi i casi indicati dall'art. 511. Il verbale predetto può quindi essere utilizzato anche senza l'audizione dei verbalizzanti (la subordinazione della lettura e quindi della utilizzabilità al compimento di determinati esami testimoniali è prevista dall'art. 511 commi 1 e 2 cpp, solo per i verbali di dichiarazioni e delle relazioni peritali, mentre per il verbale di sequestro ha vigore, invece, il comma primo dello stesso articolo) i quali però possono essere chiamati a deporre per iniziativa delle parti.

2.9.3 OPPOSIZIONI ALL'ACQUISIZIONE E RICHIESTE DI PROVA Tutti i documenti di cui s'è parlato sono fonti di prova. La parte avversa a quella che li ha fatti acquisire ha il diritto di dedurre la controprova, diretta, e la prova contraria, indiretta, riguardo al merito, al contenuto rappresentativo del documento, al fatto rappresentato, per comprometterne o demolirne il significato dimostrativo. In tutti questi casi non si tratta che della ordinaria critica della prova che il giudice deve valutare, dando poi conto, nella motivazione della sentenza, "dei risultati acquisiti e dei criteri adottati" (art. 192 cpp) e provvedendo altresì all'indicazione delle prove poste a base della decisione e all'enunciazione delle ragioni per le quali ha ritenuto non attendibili quelle contrarie (art. 546 comma 1 lettera e) cpp). La parte può rivolgere però la sua attenzione – in via preliminare rispetto alla contestazione del contenuto del documento informatico – alle modalità di acquisizione dello stesso, allo scopo di dimostrarne l'inaffidabilità e avendo di mira il risultato di escluderne l'utilizzabilità. Questo comportamento processuale trova giustificazione e fondamento nelle già ricordate volatilità e fragilità del dato informatico (che costituiscono anche il presupposto della novella introdotta dalla legge n. 48 del 2008), e cioè nelle caratteristiche che, durante la procedura di acquisizione, rendono concreto il pericolo di modificarlo, alterarlo o danneggiarlo anche involontariamente. Il rilievo si basa pertanto sull'asserita mancanza dell'adozione, per la raccolta dei dati digitali, di procedure tecniche corrette, idonee, sicure e che garantiscano che l'operazione non determini trasformazioni o contaminazioni. Naturalmente colui che lamenta che nella raccolta dei dati digitali non siano stati raggiunti i risultati imposti dalle recenti modifiche e integrazioni alle norme del codice di procedura che concernono il tema (la conformità dei dati acquisiti a quelli originali, l'inalterabilità e la conservazione di questi ultimi) ha l'onere di indicare gli elementi sui quali è fondata l'eccezione, i dati di fatto che configurano la violazione e la fase delle procedure durante la quale si sarebbe verificata l'alterazione. Ed ha interesse a fornire gli elementi di giudizio che la facciano ritenere sussistente, indicando e allegando linee guida, regole tecniche e protocolli comunemente accettati dagli ambienti scientifici, e deducendo che essi sono stati violati nel corso della raccolta della prova e hanno determinato una precisa distorsione del dato informatico. E ciò perché bisogna tenere presente che i metodi idonei per il corretto esame della memoria di un computer sono numerosi; e che se anche il metodo usato dalla pg dovesse essere ritenuto non conforme ad alcuna pratica conosciuta, tale circostanza sarebbe irrilevante senza la prova di una alterazione concreta dei dati.

2.9.4 AMMISSIONE DEL DOCUMENTO INFORMATICO E ATTIVITA' ISTRUTTORIA L'art. 190 cpp stabilisce che il giudice deve ammettere le prove richieste dalle parti solamente se esse non siano "manifestamente superflue o irrilevanti". Se, al momento dell'esame preliminare all'ammissione delle prove in dibattimento, non risultino evidenti le gravi manchevolezze della prova documentale informatica indicate dalla parte che le eccepisce, il giudice deve accogliere la richiesta di ammissione. Sarà riservata infatti a una fase successiva – e cioè al momento della valutazione del compendio probatorio acquisito nell'istruzione dibattimentale ed in vista dell'adozione del provvedimento definitivo – la decisione riguardante la fondatezza dell'eccezione di inadeguatezza della documentazione informatica affetta da tare concernenti il procedimento di acquisizione o di conservazione dei dati. Un primo elemento dell'istruttoria dibattimentale può essere rappresentato dall'audizione dell'ufficiale di pg che ha eseguito il sequestro del computer, al quale in un primo momento verrà probabilmente

chiesta la descrizione delle attività che ha compiuto per acquisire la prova. Le parti potrebbero poi chiedere allo stesso teste di esporre le sue osservazioni tecnico-scientifiche sulle varie operazioni eseguite (sequestro, estrazione di copia dell'hard disk, perquisizione dello stesso, estrazione di copia dei file rilevanti per le indagini) allo scopo di accertare la correttezza delle procedure, contestata dall'imputato. Si afferma che la deposizione degli appartenenti alla pg contenente apprezzamenti personali di natura tecnico-scientifica sia, nella sostanza, assimilabile a una perizia tecnica, e che per tale circostanza stravolgerebbe i limiti che la legge prevede per la testimonianza e realizzerebbe la situazione di incapacità a testimoniare delineata dall'art. 197 comma 1 lettera d) cpp. La Corte di Cassazione è però di opinione nettamente contraria. Il suo costante orientamento, adottato anche durante la vigenza del precedente codice di procedura afferma che "il divieto di apprezzamenti personali, previsto dall'art. 194 cpp, non è riferibile ai fatti che siano stati direttamente percepiti dal teste, al quale, a causa della speciale condizione di soggetto qualificato, per le conoscenze che gli derivano dalla sua abituale e specifica attività, non può essere precluso di esprimere apprezzamenti, se questi sono inscindibili dalla deposizione sui fatti stessi". La stessa Corte ha anche precisato che il divieto di esprimere apprezzamenti personali previsto dall'art. 194 cpp "non vale qualora il testimone sia una persona particolarmente qualificata, che riferisca su fatti caduti sotto la sua diretta percezione sensoriale e inerenti alla sua abituale e particolare attività, giacché in tal caso l'apprezzamento diventa inscindibile dal fatto". Si deve ritenere quindi che l'ufficiale di pg, oltre che descrivere in fatto le operazioni che ha eseguito per acquisire il documento informatico fonte di prova, se abbia le necessarie capacità può integrare quelle indicazioni con considerazioni di carattere tecnico-scientifico circa la loro adeguatezza e rispondenza alle esigenze desumibili dalle norme codicistiche riguardanti la conformità dei dati acquisiti a quelli originali, la conservazione e l'assenza di alterazione degli stessi. L'eventuale mancanza di consulenze di parte, contrarie al contenuto della deposizione dell'ufficiale di pg, può portare il giudice ad accogliere la tesi della correttezza delle operazioni di computer forensics senza dar corso alla nomina di un perito sull'argomento. Ma può accadere, ed è l'ipotesi normale, che il consulente della parte contrasti il contenuto tecnico della deposizione del teste. Il giudice anche in questo caso può decidere senza avvalersi dell'opera di un perito, se ritenga convincente il testimone o, al contrario, il consulente di parte. Oppure può disporre perizia. Che potrà avallare le dichiarazioni del teste, o le argomentazioni del consulente, o magari fornire una diversa ricostruzione dello svolgimento delle operazioni anche dal punto di vista tecnico. Nei casi più complessi e in quelli più delicati si può disporre una seconda perizia, magari collegiale, che può eventualmente discostarsi da tutte le osservazioni tecniche e scientifiche formulate in precedenza.

2.9.5 LA VALUTAZIONE DELLA PROVA INFORMATICA In tutte le ipotesi ora riferite si pone comunque il problema della valutazione della prova scientifica che, nel caso di quella informatica, riguarda il controllo delle operazioni eseguite dalla pg allo scopo di accertare che siano state utilizzate procedure tecnico scientifiche atte a garantire che i dati acquisiti siano conformi a quelli originali e che per gli uni e gli altri sia stata assicurata l'immodificabilità. In linea generale, il sempre più frequente ricorso a saperi specialistici comporta il rischio di affidare all'esperto, al tecnico, competenze valutative e decisionali appartenenti necessariamente all'organo giudicante. L'apprezzamento della prova scientifica si differenzia da quello delle prove tradizionali perché per queste ultime gli strumenti di valutazione sono patrimonio comune di tutti i giudici e consistono nelle massime d'esperienza, nei fatti notori e nel senso comune. Ciò non avviene nella prova scientifica dato che chi giudica raramente è munito dello specifico bagaglio culturale per valutarla. Una tale linea di tendenza finisce con l'affidare la decisione del processo al responso insindacabile di un tecnico, dato che né il giudice né le parti sono in possesso delle conoscenze necessarie per esercitare una sufficiente forma di controllo. E sussiste il pericolo che essa si trasformi in una specie di intoccabile prova legale. È questo il "paradosso della prova scientifica", che rischia di affidare la soluzione di una controversia al parere di un perito che dovrebbe essere controllato da chi (parti e giudice) non è in grado di esercitare il potere di sindacato perché manca delle necessarie conoscenze tecnico-scientifiche. Il giudicante, invece, per conservare il ruolo di garante che l'ordinamento gli assegna, non può accettare passivamente le risultanze dell'opera dell'esperto, ma deve valutare criticamente la validità e l'attendibilità delle procedure e delle conoscenze di natura scientifica adottate perché possa, a ragion veduta, condividerle o disattenderle. E così deve sindacare le tesi tecniche esposte dall'ufficiale di pg, dal consulente di parte, dal perito e anche i ragionamenti e le conclusioni dell'eventuale collegio peritale. Quali sono i mezzi con i quali chi giudica può far fonte a questo suo dovere? È certo che non può diventare egli stesso uno scienziato e ripetere esperimenti, analisi e tutto ciò che è necessario per controllare l'opera del tecnico (anche per il principio del divieto di utilizzazione della scienza privata); né può ordinare una perizia che valuti la bontà scientifica del lavoro del primo esperto: l'inconveniente si sposterebbe solamente un po' più avanti. Il giudice deve, invece, limitarsi a controllare la validità dei metodi usati dal testimone-tecnico, dal consulente e dal perito. A questo fine la letteratura giuridica richiama l'applicabilità di alcuni criteri individuati dalla Corte Suprema degli Stati Uniti nella sentenza Daubert (causa Daubert contro Merrell Dow Pharmaceuticals Inc., 1993), criteri che consistono nella controllabilità e falsificabilità del metodo scientifico, nell'avvenuto controllo della teoria da parte di esperti, nell'indicazione del margine di errore conosciuto, nell'accettazione da parte della generalità degli studiosi della materia. Per adempiere a quell'impegnativo compito il giudice deve sollecitare il contraddittorio delle parti sulla questione e deve avvalersi delle informazioni e delle notizie che possono fornirgli le stesse parti, il perito e i consulenti. In sostanza egli potrà rifarsi al semplice e

sicuro metodo per l'interpretazione delle prove scientifiche proposto in passato secondo il quale il giudicante deve verificare l'attività dell'esperto secondo quanto potrebbe fare la società civile cui appartiene, applicando i criteri della valutazione del prestigio scientifico dell'esperto, dell'accettazione generalizzata da parte degli studiosi della materia, dell'affidabilità logica della sua dissertazione. Sulla valutazione della prova informatica, sul giudizio circa l'utilizzo da parte della P.G. di procedure che non abbiano modificato i dati originali, possono poi avere influenza due elementi di giudizio: la pratica impossibilità di dimostrare l'avvenuto mutamento di quei dati e, d'altro canto, l'orientamento consolidato della Corte di Cassazione riguardo all'indeformabilità dei dati contenuti in un supporto informatico, se l'estrazione di essi sia stata curata da personale esperto. Dopo aver compiuto l'esame concernente la procedura tecnico-scientifica utilizzata per l'acquisizione del documento informatico, il giudice deve concludere dichiarandola affidabile oppure inattendibile. Se si è convinto che non siano state osservate le garanzie di correttezza pretese dalla novella di cui alla legge 18/3/2008 n. 48 a causa dell'inaffidabilità della procedura tecnica di acquisizione dei dati, egli deve necessariamente ritenere che la prova documentale sia stata ammessa, in sede di atti introduttivi al giudizio, in violazione di un divieto stabilito dalla legge (considerato che la prova fondata su un metodo scientifico insicuro è da ritenere irrilevante e pertanto inammissibile a norma dell'art, 190 comma 1 cpp) e deve dichiararla inutilizzabile alla luce del disposto dell'art. 191 primo comma cpp. Se ritiene che il dato digitale sia stato, invece, acquisito correttamente, deve procedere all'esame del contenuto del documento e alla sua valutazione alla luce dei criteri ordinari di apprezzamento del quadro probatorio (artt. 192 comma 1 e 546 comma 1 lettera e) cpp). Tutto il ragionamento probatorio deve essere esposto nella motivazione della sentenza, che deve contenere una puntuale ed esauriente indicazione di ciò che il giudicante ha esaminato, dei criteri che ha utilizzato per decidere come ha deciso, nonché la spiegazione dei motivi per i quali ha ritenuto esatta una tesi e infondata quella contraria, alla luce, del resto, di quanto affermano gli artt. 192 comma 1 e 546 comma 1 lettera e) del codice di procedura penale. Per quanto riguarda la prova informatica in particolare, il giudice deve riferire le informazioni scientifiche che ha esaminato e deve fornire una convincente, completa e comprensibile spiegazione dell'apprezzamento compiuto.

2.9.6 POTENZIALITÀ PROBATORIE DELLA DIGITAL EVIDENCE Ci si può chiedere quali siano le capacità di accertamento del documento informatico riguardo all'oggetto della prova, quale risulta dalla descrizione che ne dà l'art. 187 cpp. Si potrebbe supporre che la prova scientifica, "si presenti con credenziali di particolare attendibilità e forza persuasiva rispetto agli standard ordinari del giudizio penale". E invece la prova informatica ha una caratteristica negativa quanto alla sua attitudine probatoria, essendo risaputo che quasi sempre il dato contenuto nel computer dimostra con sicurezza solamente il lasso di tempo nel quale questo è stato usato, ma non contiene elementi che permettano di accertare l'identità della persona che stesse adoperando la macchina in quei momenti rilevanti ai fini del processo. È anche noto che nelle attività informatiche vengono adoperate tecniche per garantire l'anonimato dell'operatore o la sostituzione d'identità; per confezionare false credenziali oppure alterare il contenuto delle operazioni del computer; per introdursi in un sistema con un trojan e condizionarlo a eseguire programmi solo formalmente riconducibili al possessore, oppure introdurre immagini o altri contenuti nella memoria dell'apparecchio. Queste caratteristiche degli strumenti digitali determinano il valore meramente indiziario delle informazioni derivanti dalle indagini che li utilizzano come fonte di prova. Sorge, di conseguenza, la necessità di confortare le investigazioni informatiche con tutti i sistemi di indagine ampiamente utilizzati, collaudati, di carattere tradizionale (pedinamenti, esame di persone informate sui fatti, rilevazione di impronte digitali sulla tastiera, ecc.). E tale circostanza rende fondata l'affermazione secondo la quale "l'inchiesta penale classica può spesso fare a meno della computer forensics, mentre quest'ultima possiede un margine di autonomia dimostrativa molto esiguo". Si può concludere citando una affermazione, insieme etica e giuridica, formulata dalla Corte di Cassazione, secondo la quale bisogna approdare a "un concetto più volte scandito dalla giurisprudenza di legittimità, cioè all'infungibilità del ragionamento probatorio che ha, nei margini di una corretta, prudente e giustificata discrezionalità, una connotazione di compiutezza. Non esiste nella concezione del nostro legislatore l'idea del miracolo tecnologico quale ultimo e magico supporto di una decisione tormentata e impossibile. Alla base di certe scelte tecniche c'è sempre l'uomo-giudice, che ha solo il bisogno, eventualmente, d'integrare certe sue conoscenze tecniche per decidere, ma per decidere con la sua testa", perché, continua la Corte "non ci sono deroghe al libero convincimento del giudice nell'ambito di un rigoroso riscontro della logicità della sentenza".

3. Conclusioni La prova scientifica e in particolare quella informatica, rivestono una sempre maggiore importanza nel processo penale e hanno l'effetto di restringere i poteri di valutazione delle prove da parte del giudice, che si avviano ad essere sostituiti dal parere del tecnico, insindacabile da chi non abbia le stesse particolari cognizioni. Il computer è uno strumento divenuto indispensabile nella società attuale, ma rappresenta anche un congegno che serve per la commissione di reati, o che ne costituisce l'oggetto. Molte volte esso è anche il contenitore di notizie relative ad attività delittuose. La gigantesca memoria dell'elaboratore è particolarmente delicata perché i dati immateriali che contiene possono essere facilmente danneggiati, anche solamente per imperizia. Si pone pertanto il problema dell'acquisizione, da parte della pg, del materiale probatorio archiviato, mediante procedure che garantiscano la genuinità e la affidabilità dello stesso e quindi la sua utilizzabilità nel processo penale.

La legge 18/2/2008 n. 48 ha aggiornato il codice di procedura penale riguardo alle indagini relative all'utilizzo dell'informatica per il perseguimento dei reati. La novella legislativa, senza dettare un regolamento per la ricerca e l'apprensione sicura delle prove informatiche, ha indicato le esigenze che l'attività d'indagine deve soddisfare: assicurare la conservazione dei dati originali; impedirne l'alterazione; garantire la conformità della copia degli stessi elementi a quelli originali, la loro non modificabilità. Secondo l'orientamento consolidato della Corte di Cassazione, le operazioni di prelievo del contenuto delle memorie informatiche non danno luogo a un accertamento tecnico irripetibile – e quindi non richiedono l'applicazione delle procedure e delle garanzie previste dall'art. 360 cpp – se eseguite da personale esperto, perché si crede che l'operazione sia riproducibile illimitatamente. Una parte della dottrina afferma che fra i presupposti per disporre perquisizione e sequestro della memoria di un computer ci sarebbe anche quello di individuare preventivamente e specificamente che cosa debba essere cercato e sequestrato, di modo che sia acquisito solamente il materiale che strettamente riguardi il reato ipotizzato e si possa così evitare che la pg prenda cognizione di molti altri dati estranei all'indagine, in violazione dei diritti alla riservatezza dell'individuo. Secondo la giurisprudenza della Corte Suprema, invece, non si può pretendere che il provvedimento predetto contenga l'indicazione dettagliata delle cose, o dei file, da ricercare e sequestrare, poiché esso può limitarsi a ordinare genericamente la ricerca e la sottoposizione a vincolo di ogni cosa che possa sembrare utile ai fini dell'indagine. In questo caso la pg ha il compito di esaminare tutto quello che rinvenga, nonché di individuare e sequestrare il materiale rilevante, salva la convalida da parte dell'ag. È stato sollevato il problema della tutela della libertà e della segretezza della corrispondenza contenuta nella memoria del computer sequestrato. Per la giurisprudenza di legittimità rientrano nel concetto tecnico giuridico di "corrispondenza", sequestrabile a norma dell'art. 254 cpp, solamente gli oggetti per i quali è in corso la spedizione; mentre sono acquisibili ai sensi dell'art. 253 cpp le lettere, i plichi, i messaggi di posta elettronica destinati alla corrispondenza oppure già recapitati al destinatario, che siano già stati aperti oppure non ancora letti, per i quali non vi sia quindi un'attività di spedizione in atto. Nel dibattimento la prova digitale entra come "documento". Spesso esso è acquisito a norma dell'art. 190 cpp mentre altre volte entra nel fascicolo per il dibattimento a norma dell'art. 431 cpp, come accade per il documento-corpo del reato e per il verbale di sequestro. Questi ultimi, per poter avere efficacia probatoria, devono essere letti a norma dell'art. 511 cpp e non è necessario che, per dare forza dimostrativa al secondo, sia necessaria l'audizione dell'ufficiale di pg che lo ha redatto. Ma è prevista la facoltà delle parti di chiedere che quell'ufficiale sia chiamato a testimoniare in merito al contenuto del verbale che ha redatto. La Cassazione afferma che, nell'occasione, quel teste, nella sua qualità di esperto, possa illustrare gli aspetti tecnico-scientifici dell'indagine informatica. Gli stessi aspetti che possono essere oggetto anche dell'attività dei consulenti di parte o del perito d'ufficio. Il giudice non può accogliere acriticamente le teorie scientifiche e i rilievi specialistici riguardanti la correttezza dell'acquisizione della prova informatica, da chiunque essi vengano illustrati in dibattimento, ma deve valutarli alla luce dei parametri individuati dalla dottrina e dalla giurisprudenza, per non lasciare al responso insindacabile di un tecnico la decisione che solo il giudice può adottare nel suo libero convincimento. Nel merito, la prova informatica non ha la capacità dimostrativa che comunemente ci si aspetterebbe da un mezzo istruttorio di carattere scientifico, che si immagina essere preciso e incontrovertibile. Esso ha, invece, quasi sempre un valore indiziario a causa delle difficoltà di accertamento dell'identità di chi adopera in un dato momento l'apparecchio digitale e anche per effetto della facilità con cui si possono falsificare i contenuti della memoria mediante tecniche sofisticate di difficile o impossibile accertamento. A causa della loro limitata efficacia probatoria gli elementi istruttori di natura informatica possono solamente concorrere a dare fondamento alla decisione, insieme con altri elementi di prova acquisiti con i tradizionali sistemi di indagine.

* vice questore aggiunto della Polizia di Stato, direttore sezione indagini elettroniche Servizio polizia scientifica

Scarica il PDF dell'inserto

01/03/2015