PROVE DIGITALI E PROCESSO: LA COMPUTER FORENSICS

SOMMARIO: 1. Computer forensics: una nuova disciplina – 2. L'acquisizione della prova digitale – 3. Le indagini difensive – 4. La perquisizione – 5. ...segue: sequestro o copia? – 6. L'analisi – 7. Procedimenti civili e computer forensics – 8. Controlli a distanza

1. L'informatica è oggi diventata, nel bene e nel male, uno strumento irrinunciabile della nostra vita quotidiana, lavorativa e ludica; le problematiche giuridiche sollevate dallo sviluppo dell'universo elettronico rappresentano, probabilmente, uno dei terreni di sfida culturale più stimolanti della nostra epoca laddove il processo relativo a reati informatici solleva nuove problematiche di carattere investigativo, probatorio e processuale, con la conseguenza che si sono andate formando nuove professionalità in grado di muoversi, più o meno disinvoltamente, in questa terra di confine. A questo proposito, uno dei temi che più appassionano gli esperti è proprio quello relativo al computer come "elemento di prova" da acquisire, analizzare ed utilizzare in un processo: in molti recenti procedimenti, non necessariamente relativi a reati informatici[1], il computer si è spesso rivelato un "testimone chiave" per l'accusa o per la difesa.

In realtà sarebbe più corretto, almeno formalmente, parlare del computer come "prova", se non come "fonte di prova", ma non di rado l'approccio del perito (nominato dal giudice) o del consulente (nominato da una delle parti)[2] con il computer è più simile a quello di chi interroghi un testimone reticente, piuttosto che quello di chi esamini un reperto inanimato: non basta trovare tracce del reato (o non trovarne), occorre interpretare i silenzi (i dati sono stati cancellati o non sono mai esistiti?) e, persino, le "rivelazioni" (i dati si trovano lì ad insaputa dell'imputato/indagato o vi sono stati consapevolmente collocati da lui?).

Proprio per questa ragione l'analisi forense di un computer non dovrebbe mai ridursi ad un "positivo" o ad un "negativo", ma dovrebbe sempre essere adeguatamente supportata da motivazioni logiche, soprattutto in presenza di reati

[1] Si pensi, ad esempio, il ruolo ricoperto dal computer dell'imputato in alcuni recenti casi di cronaca relativi a procedimenti penali per omicidio.

[2] Per comodità espositiva, nelle pagine che seguono si parlerà genericamente di "consulente". Salvo differente indicazione, con tale termine andrà inteso il consulente del PM, quello della difesa, il perito nominato dal Giudice ed anche l'ausiliario di PG nominato ai sensi dell'art. 348 c.p.p

particolarmente odiosi quali quelli di detenzione, cessione o divulgazione di pornografia minorile.

L'indagine non può, quindi, essere ridotta ad attività meramente informatica, in quanto il consulente dovrebbe sempre cercare di ricostruire il comportamento tenuto dall'imputato di fronte al computer, arrivando ad interpretare i risultati dell'analisi alla luce di tale ricostruzione comportamentale, soprattutto, al fine di valutare se un determinato atto sia stato compiuto consapevolmente e volontariamente oppure per ignoranza o inesperienza.

Non può, poi, non avvertirsi l'esigenza di regole comuni e di procedure certe, in assenza delle quali è molto difficile riuscire a garantire un sereno rapporto tra accusa e difesa nella dialettica processuale e preprocessuale. Mai come oggi, infatti, si avverte la necessità della "certezza delle regole", soprattutto per quanto riguarda l'individuazione e la conservazione di quei dati che poi costituiranno l'oggetto su cui si fonderà la valutazione dell'organo giudicante.

Il rilevamento, la conservazione ed il trattamento di questo materiale e delle informazioni che gli investigatori (ma anche, non dimentichiamolo, i difensori) possono rilevare nel normale svolgimento dell'attività d'indagine esigono un protocollo operativo che ne garantisca integrità e non repudiabilità in sede processuale[3].

La *computer forensics* si presenta, quindi, come una scienza complessa, multidisciplinare e, proprio per questo, estremamente intrigante.

2. L'indagine relativa ai reati informatici dipende in gran parte dal tipo di crimine che si vuole reprimere: siccome diverse sono le tracce lasciate dagli autori ad esse devono adattarsi le modalità investigative anche in ragione del fatto che diversi sono gli strumenti forniti dal legislatore.

Alcune caratteristiche, tuttavia, prescindono dall'illecito commesso e possono essere ritenute comuni alle varie, differenti tipologie di indagine; *in primis* la fase di acquisizione delle prove e delle informazioni deve essere il più possibile celere

[3] In tal senso si veda B. FIAMMELLA, *Problematiche giuridiche in tema di computer forensic,* Sintesi dell'intervento svolto durante il Convegno Internazionale "Pedofilia on-line: strategie di contrasto e di prevenzione", Roma, Aula Magna del Ministero delle Comunicazioni, 8 luglio 2004, in FIAMMELLA.it; G. COSTABILE, *Scena criminis, documento informatico e formazione della prova penale*, in convegnovarenna.giuristitelematici.it; D. FORTE, *Le attività informatiche a supporto delle indagini giudiziarie*, in Rivista della G. di F., n°2, 2000, p. 541

dato che poche cose sono volatili come le evidenze informatiche: basta davvero poco per alterarle, modificarle o renderle comunque inservibili, sia volontariamente che involontariamente.

In secondo luogo, l'investigatore deve essere in grado di ricostruire il prima possibile e con la maggiore precisione le modalità con cui è stato commesso il reato, anche al fine di valutare adeguatamente la genuinità di eventuali prove raccolte, ovvero di scagionare eventuali coimputati[4].

A ciò deve aggiungersi che in questa fase, in cui l'indagato è generalmente all'oscuro delle indagini, possono essere disposte intercettazioni telefoniche, informatiche o ambientali, eseguite ispezioni e perquisizioni al fine di acquisire elementi di prova da poter utilizzare successivamente, svolte attività sotto copertura (accesso a siti, contatti in chat, scambio di materiale attraverso le reti p2p); si tratta di attività che devono seguire dei rigidi protocolli procedurali, la cui violazione potrebbe ben determinare l'inutilizzabilità in sede dibattimentale delle prove eventualmente acquisite.

E' bene ricordare che, in questa fase, non vi è ancora nessun obbligo formale di avvisare l'indagato della sua posizione, ma questi, se ha il sospetto della pendenza di indagini sul suo conto, può presentare un'istanza presso la Procura della Repubblica per sapere se vi sono procedimenti penali a suo carico[5]. In caso positivo, questi gli devono essere comunicati, salvo che l'indagine riguardi reati particolarmente gravi ovvero tale informazione sia stata secretata dal PM, con decreto motivato[6], ma, in quest'ultimo caso, il periodo non può superare i tre mesi.

---

[4] In tal senso si veda la motivazione del Tribunale Penale di Bologna, sez. I monocratica, sentenza 21 luglio 2005 (dep. 22 dicembre 2005), est. di Bari. "*... L'esclusiva assunzione di responsabilità da parte del fratello G., come si è sopra detto, è invece riscontrata sia dalla riferibilità a lui delle operazioni di amministrazione dei due siti internet, sia dal possesso – che non risulta avere il fratello - delle idonee capacità di programmazione: del resto i programmi sequestrati presso la comune residenza familiare furono trovati nei dischi rigidi presenti nella stanza nella disponibilità esclusiva di G.*". In relazione agli elementi "ambientali" si veda anche Cass. pen., sez. III, 11 marzo 2010, n. 15100 "*...nella abitazione vi era un solo p.c, precisamente nella camera da letto del prevenuto, a cui era intestato l'abbonamento internet*".

[5] Richiesta ai sensi dell'art. 335 c.p.p.

[6] Art. 335 c.p.p. "*3. Ad esclusione dei casi in cui si procede per uno dei delitti di cui all'articolo 407, comma 2, lettera a), le iscrizioni previste dai commi 1 e 2 sono comunicate alla persona alla quale il reato è attribuito, alla persona offesa e ai rispettivi difensori, ove ne facciano richiesta.*

3 bis. Se sussistono specifiche esigenze attinenti all'attività di indagine, il pubblico ministero, nel decidere sulla richiesta, può disporre con decreto motivato, il segreto sulle iscrizioni per un periodo non superiore a tre mesi e non rinnovabile.

3. In ogni caso, anche in assenza dello status di imputato o indagato, è possibile svolgere indagini difensive in via preventiva, ad esclusione degli atti che richiedono l'intervento dell'autorità giudiziaria e purché il difensore abbia ricevuto un apposito mandato che indichi espressamente i fatti ai quali si riferisce.

Per esempio, a seguito di uno scambio di insulti in un forum Tizio sospetta che Caio possa averlo querelato, incarica allora il proprio difensore di fiducia di svolgere attività investigativa preventiva al fine di acquisire tutti quegli elementi che potrebbero rivelarsi utili per la futura difesa; in questo modo il difensore potrà individuare e sentire eventuali testimoni con lo strumento del colloquio, della ricezione di informazioni, tramite l'assunzione di informazioni e/o acquisire documenti di vario genere[7], che potranno essere validamente utilizzati in sede di giudizio.

In questo, come in altri casi, l'attività preventiva potrebbe rivelarsi particolarmente utile, magari per decidere se presentare o meno una querela ovvero per rispondere alla stessa allegando eventuali elementi probatori in grado di suffragare la propria versione dei fatti, dimostrando di essere stati vittime di una provocazione da parte della controparte, ovvero per individuare con maggiore sicurezza elementi di prova a difesa (i.e. si pensi all'ipotesi di messaggi inviati ad un gruppo di discussione attivando l'opzione x-noarchive=yes, che determina la cancellazione del messaggio dopo pochi giorni). Non può, però, trascurarsi un concreto pericolo insito nell'attività di indagine preventiva, relativo alla tutela di un terzo che si trovi ad essere "indagato" da un privato nell'ambito di un'indagine privata.

Quali garanzie potranno, infatti, essere assicurate al cittadino, coinvolto nello svolgimento di atti finalizzati alla ricerca (ed alla formazione) di prove a suo carico, allorquando queste vengono raccolte e collezionate non da un pubblico ufficiale, ma da un altro privato cittadino? Questi, infatti, non soltanto non avrà alcun obbligo di informazione nei confronti del sospetto, che, non essendo iscritto nel registro degli indagati, non godrà di nessuna delle garanzie legate al relativo status, ma, a differenza del Magistrato e della PG, non avrà neppure alcun obbligo di individuazione e raccolta di eventuali prove a discarico né, tanto meno, quello

[7] Art. 391 *bis* e seguenti c.p.p.

di documentare ed allegare tutte le attività svolte durante le indagini, ma soltanto quel materiale di cui intenda fare uso in sede processuale[8]!

Il pericolo è concreto, soprattutto nel processo penale innanzi al giudice di pace, ove è possibile immaginare la presenza di un'"accusa privata" in grado di raccogliere le prove, formulare l'ipotesi accusatoria e, persino, citare a giudizio l'imputato[9].

L'analisi delle conseguenze di tale situazione, esula dalla portata del presente lavoro, ma è significativa in relazione al livello di attenzione e professionalità che dovrà essere richiesto al difensore/accusatore ed ai suoi ausiliari, siano essi consulenti tecnici o investigatori privati.

Si tratta di figure professionali che escono particolarmente rafforzate dalla riforma e che, di fatto, si collocano a fianco del difensore per coadiuvarlo nello svolgimento delle indagini difensive, ricoprendo, sia pure con le dovute differenze, un ruolo speculare a quello della polizia giudiziaria.

---

[8]In tal senso si veda F.M. GRIFANTINI, "TUTTI I NODI VENGONO AL PETTINE: L'INCOGNITA DEL DIFENSORE-ISTRUTTORE TRA MITI E REALTà", in *Cass. pen*., 2004, 01, 395 secondo cui "*Il pubblico ministero è obbligato a compiere atti, a documentarli nelle forme per essi previste e, alla fine delle indagini, a depositarne i risultati, che sono utilizzabili da subito. Il difensore compie atti da impiegare secondo scelte strategiche, in quanto non solo non è obbligato a svolgere indagini, ma non è tenuto a documentarle (nel senso che si tratta di un onere per la difesa la quale intenda utilizzarle), né ad inserire i risultati nel procedimento: sceglie se avvalersene o meno a seconda della convenienza per i propri fini, dal momento che producendo prove a carico dell'assistito rischierebbe addirittura di commettere reato (art. 380 c.p.)*". Si veda anche Cassazione penale, sez. un., 27 giugno 2006, n. 32009 "*Evidente è la differenza funzionale tra il P.M. e la difesa, in quanto solo il primo è tenuto a raccogliere tutte le emergenze riguardanti l'indiziato mentre al secondo la legge riconosce poteri ampiamente dispositivi. Per attribuire però al difensore, in fase di documentazione delle indagini, la veste pubblica non occorre passare per la dimostrazione della parità dei doveri e dei poteri rispetto al P.M.*.

E' vero che il difensore non ha il dovere di cooperare alla ricerca della verità e che al professionista è riconosciuto il diritto di ricercare soltanto gli elementi utili alla tutela del proprio assistito, però sicuramente non gli è riconosciuto il diritto di manipolare le informazioni ricevute ovvero di selezionarle verbalizzando solo quelle favorevoli. L'interesse dell'Avvocatura, del resto, non può che essere quello di rendere la prova dichiarativa assunta dal difensore affidabile al pari di quella raccolta dall'accusa, mentre la tutela difensiva resta assolutamente integra e non riceve compromissione alcuna attraverso il riconoscimento legislativo della possibilità di non fare seguire al colloquio preventivo la sua verbalizzazione, nonchè di omettere di utilizzare processualmente il verbale di dichiarazioni che contenga elementi sfavorevoli (art. 391 octies c.p.p.)".

[9] L'art.25 del D.Lgs 274/2000 prevede che l'azione penale venga comunque esercitata dal PM che "*entro dieci giorni dalla comunicazione del ricorso [...] presenta le sue richieste nella cancelleria del giudice di pace.*

Se ritiene il ricorso inammissibile o manifestamente infondato, ovvero presentato dinanzi ad un giudice di pace incompetente per territorio, il pubblico ministero esprime parere contrario alla citazione altrimenti formula l'imputazione confermando o modificando l'addebito contenuto nel ricorso.".

L'articolo 21, comma 2, lett.f), impone, in ogni caso, al ricorrente l'onere di indicare nel ricorso "*la descrizione, in forma chiara e precisa, del fatto che si addebita alla persona citata a giudizio, con l'indicazione degli articoli di legge che si assumono violati*".

Con la legge del 2000 si è, in primo luogo, equiparata la posizione degli ausiliari a quella del difensore, laddove l'articolo 103, comma 2, del codice di procedura ora stabilisce che "*presso i difensori e gli investigatori privati autorizzati ed incaricati in relazione al procedimento nonché presso i consulenti tecnici non si può procedere a sequestro di carte o documenti*...".

Allo stesso modo l'articolo 200 c.p.p. consente, anche all'investigatore privato autorizzato ed al consulente, di opporre il segreto professionale, mentre l'articolo 334 *bis* stabilisce espressamente che il difensore ed i suoi ausiliari non hanno alcun obbligo di denuncia "*neppure relativamente ai reati dei quali hanno avuto notizia nel corso delle attività investigative da essi svolte*".

In quest'ottica, è di assoluta importanza, soprattutto in presenza di reati tecnologici, che l'avvocato si avvalga di un consulente di fiducia, che sia anche in grado di indirizzarlo verso determinati atti di indagine difensiva. Il consulente, al pari dell'investigatore, può essere nominato in qualsiasi momento, ma è importante che la sua nomina venga formalizzata, affinché lo stesso possa opporre il segreto professionale alle domande degli inquirenti.

Del pari l'investigatore privato dovrà possedere nuove e più specialistiche competenze, che lo mettano, per esempio, in grado di acquisire elementi di prova senza inquinarli ovvero di interrogare testimoni nella maniera più efficiente possibile, evitando anche soltanto il sospetto della subornazione.

4. In generale, tuttavia, il soggetto scopre di essere indagato nel momento in cui riceve la famigerata "informazione di garanzia" che, nel caso di reati informatici, tipicamente, ma non sempre, viene notificata congiuntamente ad un decreto di perquisizione e sequestro.

È comunque sempre possibile che un soggetto possa subire una perquisizione senza aver ancora assunto formalmente lo *status* di indagato; il caso di scuola è rappresentato dalla perquisizione presso terzi, tipicamente nel caso di indagini a carico di ignoti oppure nel caso in cui l'autore del reato non sia il proprietario del bene sequestrato (per esempio un dipendente commette un reato informatico con il computer dell'ufficio).

Si tratta di ipotesi sempre più frequenti, laddove la prassi di aprire un

procedimento nei confronti di ignoti rappresenta la soluzione giuridicamente più corretta nella maggior parte dei reati informatici quando l'alternativa è quella di iscrivere *tout court* al registro degli indagati il titolare dell'utenza telefonica utilizzata per commettere il reato, individuata sulla base dell'indirizzo IP utilizzato al momento del fatto dall'autore dell'illecito.

E' appena il caso di notare che una simile soluzione appare, se non scorretta da un punto di vista strettamente giuridico, quantomeno ingiusta nei confronti di un soggetto che si troverebbe ad essere indagato per il semplice fatto di aver stipulato un contratto, ma, è appena il caso di ricordarlo, mentre nel diritto civile vi sono varie forme di responsabilità per fatto altrui, la responsabilità penale è strettamente personale e non possono esistere forme di responsabilità penale oggettiva.

Si pensi alla classica situazione in cui si trovano migliaia di studenti universitari: più studenti convivono in un appartamento ed uno si intesta il contratto di locazione mentre un altro l'utenza telefonica. Se uno dei coinquilini commette un reato, chi deve essere iscritto nel registro degli indagati?

E' di tutta evidenza che, in una prima fase, nessuno dovrebbe essere formalmente indagato, pertanto, almeno fino alla perquisizione, si dovrebbe procedere nei confronti di ignoti e poi, in quella sede o successivamente, cercare di capire chi, tra i coinquilini, ha commesso il reato. E' ovvio che, non appena la figura del responsabile inizia a delinearsi, questi deve, senza indugio, essere iscritto nel registro degli indagati ed acquisire i relativi diritti.

Ovviamente non si tratta dell'unica strada percorribile, dato che è ben possibile iscrivere tutti i coinquilini al registro degli indagati e, come avrebbe detto Amaury, lasciare che sia poi Dio a riconoscere i suoi...

In ogni caso la perquisizione rappresenta un momento fondamentale dell'indagine, soprattutto per la labilità e la deperibilità delle prove informatiche: eventuali reperti non individuati in prima battuta sono probabilmente destinati a sparire in maniera definitiva.

In breve, la perquisizione è la sede dove devono essere compiute quelle operazioni in grado di “cristallizzare” le prove, evitando ogni possibile contaminazione degli elementi probatori: per esempio, è necessario evitare di

accendere i computer trovati spenti e ponderare bene se, come e quando spegnere quelli trovati accesi. Laddove possibile, sarebbe poi opportuno annotare con cura, eventualmente anche scattando fotografie o utilizzando una videocamera, la disposizione degli apparati all'interno dell'ufficio o dell'abitazione: oggetti a prima vista insignificanti possono rappresentare un'ottima fonte di informazioni o, addirittura, essere elementi di prova: il mouse era a destra o a sinistra?

In questa fase l'imputato, ma anche chi abbia la materiale disponibilità dei luoghi, ha la facoltà di farsi assistere o rappresentare da una persona di fiducia "purché prontamente reperibile e idonea"; già in questa fase è quindi possibile nominare il proprio difensore e, eventualmente, richiederne l'intervento in loco.

Per quanto riguarda gli orari, le perquisizioni presso il domicilio devono essere svolte tra le ore 7:00 e le ore 20:00[10], salvo casi di particolare urgenza in cui l'autorità giudiziaria può disporre, per iscritto, che le operazioni vengano svolte al di fuori di questi termini temporali.

Una volta sbrigate tutte le formalità, si procede alla ricerca degli elementi di prova ed all'acquisizione dei supporti informatici e, di nuovo, ci si imbatte in un ulteriore problema metodologico: come comportarsi nel caso in cui il computer sia acceso al momento dell'accesso?

In caso di computer spento, infatti, la procedura è, relativamente semplice: si prende l'hard disk, si effettua un'immagine dello stesso, si acquisisce il relativo hash, lo si annota nel verbale e si imballa l'originale, preferibilmente apponendo i sigilli alla scatola.

Una volta eseguite queste operazioni e laddove ve ne sia la possibilità, è sempre buona norma verificare che l'hard disk (la copia non l'originale!) sia leggibile e che non vi siano nel PC schede particolari, in grado di inibire l'accesso allo stesso. A tal proposito è assai utile la lettura dei manuali delle schede o del sistema, ovvero una verifica tramite internet delle caratteristiche dei componenti. In caso di dubbio è opportuno prelevare tutto il materiale spiegandone, all'interno del verbale di sequestro, le ragioni.

Sempre più spesso, però, i PC rimangono costantemente accesi e, magari, con vari programmi in esecuzione; cosa fare, dunque, in caso di computer in funzione?

[10] Art. 251 c.p.p.

La soluzione ottimale sarebbe quella di poter disporre, direttamente in sede di perquisizione, di un soggetto con adeguata competenza che, alla presenza della parte, possa analizzare (con le modalità proprie dell'ispezione) la macchina accesa, verificarne i processi in esecuzione e procedere infine al suo spegnimento, annotando e riprendendo tutte le operazioni eseguite; tuttavia, nel caso in cui ciò non fosse possibile, ovvero non si sia certi dell'assenza di sistemi di sicurezza particolari, la soluzione pratica migliore è indubbiamente quella di staccare direttamente la spina dal computer, procedendo anche alla rimozione delle batterie in caso di computer portatile[11].

Tralasciamo, per semplicità, l'ipotesi in cui si rilevi la presenza di partizioni o dischi virtuali in *mount*: questa fattispecie richiede un approccio completamente differente dato che necessario procedere con l'ispezione della macchina direttamente in loco e l'acquisizione immediata del contenuto del disco virtuale, o della macchina virtuale; è assai probabile, infatti, che, al successivo riavvio, sarà necessaria una o più password per avviarli e, è bene ricordarlo, l'imputato non può essere costretto a consegnare agli inquirenti la propria password.

5. *In primis*, si deve osservare che anche il sequestro di materiale apparentemente inutili (che tanta ilarità ha suscitato e continua a suscitare nelle riviste specializzate) potrebbe avere un suo valido motivo: per esempio elementi hardware come la tastiera o il mouse potrebbero, in caso di dubbio, rivelare utili elementi in ordine al loro utilizzatore (impronte digitali, frammenti di pelle, tracce di fluidi corporei...) e lo stesso, vituperato, tappetino del mouse potrebbe contenere informazioni interessanti di natura biologica (per non parlare delle volte in cui sul retro dello stesso sono annotate password o altre informazioni utili!); non possiamo né dobbiamo, infatti, dimenticare che l'ambiente "informatico" non è il solo e l'unico in cui è possibile trovare elementi di prova.

In questa sede, il tipico punto di scontro tra accusa e difesa è relativo alle modalità con cui si procederà al sequestro di evidenze informatiche: il nodo centrale della questione è, infatti, se, in caso di indagini per reati informatici, sia

[11] AA.VV., *Electronic Crime Scene Investigation: a guide for first responders*, a cura di U.S. Department of Justice, http://www.ncjrs.gov/pdffiles1/nij/187736.pdf. E' evidente che, in questo modo, si perderà la possibilità di acquisire i dati presenti in RAM, ma allo stato delle cose si tratta della procedura più sicura per personale inesperto.

necessario sequestrare tutto il computer, solo l'hard disk oppure se sia sufficiente acquisire una copia dei dati[12]. La questione non è di facile soluzione in quanto la scelta, fatta nella concitazione del sequestro, si riflette necessariamente nelle successive fasi predibattimentali e, spesso, anche nel dibattimento stesso, rischiando di pregiudicare l'analisi e, conseguentemente, i diritti di accusa e difesa.

In primo luogo, dobbiamo osservare che non può esserci una risposta precisa a questa domanda, in quanto a reati differenti devono corrispondere differenti tipologie di indagine, che richiedono approcci diversi e, soprattutto, una modalità di acquisizione della prova modellata sulla fattispecie concreta[13]. E' evidente che, a parità di risultato probatorio, dovrà essere necessariamente privilegiata la modalità di acquisizione meno invasiva e che comporta il minor danno per il soggetto che la subisce; soggetto che, a volte, non è neppure indagato, ma si trova nella posizione di "persona informata sui fatti"[14].

Logicamente la soluzione con il minor impatto in termini di disagi per la persona sottoposta ad indagine è l'acquisizione, direttamente in sede di ispezione/perquisizione, dei dati costituenti tracce del reato o corpo del reato ad opera della PG procedente, ma, sebbene si tratti della soluzione preferibile, da adottare ogni qual volta le circostanze la rendano possibile, presenta almeno due grossi problemi[15]:

1) richiede, per essere eseguita, la presenza di personale esperto in grado di operare, in maniera sicura, su supporti hardware e software sconosciuti e di individuare, in tempi rapidissimi tutti i file di interesse probatorio (ivi compresi quelli cancellati, crittografati o steganografati), per poi procedere alla loro cristallizzazione direttamente nel luogo in cui si trovano;
2) l'operazione, anche se eseguita secondo le *best practices* della *computer*

[12] In tal senso si veda F. MARCELLINO, *Principio di pertinenza e sequestri di computer*, in guide.supereva.com/diritto. Si veda anche A. MONTI, S. CICCARELLI, *Spaghetti hacker*, Apogeo, 1997, *passim*; G. COSTABILE, *Scena criminis, cit.*

[13] Nelle pagine che seguiranno si parlerà esclusivamente delle memorie informatiche contenute nel computer. In merito alla possibilità di sequestro di ulteriori supporti di immagazzinamento dati si rimanda alla fine del paragrafo.

[14] Sempre più spesso capita che, soprattutto per particolari tipologie di reato o in caso di più utenti della medesima connessione telefonica, si preferisca iscrivere un procedimento penale a carico di ignoti, per poi formalizzare il capo di imputazione in un secondo momento al soggetto identificato grazie all'analisi delle evidenze digitali.

[15] In tal senso si veda G. COSTABILE, *Scena criminis, cit.*

forensics, è, di fatto, irripetibile in quanto il materiale, rimasto nella disponibilità dell'imputato, deve considerarsi non più utile per finalità investigative.

In breve l'utilizzo dello strumento dell'ispezione, con la conseguente acquisizione, anche mediante masterizzazione, dei soli file pertinenti al reato, andrebbe utilizzata soltanto laddove il computer assuma la veste di mero contenitore della prova del crimine e si ritenga opportuno non operare un sequestro, per esempio perché lo si ritiene sproporzionato al fatto contestato, oppure nel caso di attività presso terzi (banche, provider, etc.) estranei di fatto alla vicenda[16].

Un caso pratico dei rischi insiti in tale procedura è rappresentato dall'eccezione della difesa, sollevata nel corso del processo all'autore del Worm Vierika[17]; in sede di perquisizione la PG si era limitata ad acquisire una copia dei soli file aventi rilevanza investigativa; più precisamente, al momento della perquisizione domiciliare, l'indagato aveva indicato alla PG operante il programma, masterizzandone le copie da sottoporre a sequestro sotto il diretto controllo degli agenti, ma, in sede processuale, la difesa eccepiva la correttezza del metodo utilizzato dalla PG per estrarre i programmi dal computer.

Il Giudice non accoglieva la tesi, pur ammettendo che le modalità di acquisizione si discostavano dalle *best practices*, osservando che "*non è permesso al Tribunale escludere a priori i risultati di una tecnica informatica utilizzata a fini forensi solo perché alcune fonti ritengono ve ne siano di più scientificamente corrette, in assenza della allegazione di fatti che suggeriscano che si possa essere astrattamente verificata nel caso concreto una qualsiasi forma di alterazione dei dati e senza che venga indicata la fase delle procedure durante la quale si ritiene essere avvenuta la possibile alterazione*"[18].

La soluzione preferibile è, dunque, rappresentata dal sequestro del solo hard disk oppure dall'acquisizione, con strumenti idonei, di un'immagine dello stesso,

[16] In tal senso si veda G. COSTABILE, *Scena criminis, cit;* G. Todesco, *L'indagine informatica di Polizia Giudiziaria: trasmissione dati su rete, perquisizioni ed ispezioni informatiche*, in marcomattiucci.it, 1998.

[17] Cfr.Tribunale Penale di Bologna, sez. I monocratica, sentenza 21 luglio 2005 (dep. 22 dicembre 2005), est. di Bari.

[18] Per una critica a questa decisione si veda L. LUPARIA, *Il caso "Vierika": un'interessante pronuncia in materia di virus informatici e prova penale digitale*, in *Diritto dell'internet*, 2006, n.2, p. 155.

laddove si ritenga opportuno lasciare l'hard disk nella disponibilità dell'imputato.

Tale soluzione, applicabile alla maggior parte dei reati informatici, consente un pieno controllo del contenuto del supporto e la ripetibilità, in qualsiasi momento, dell'analisi eseguita, ma, di contro, richiede, in sede di perquisizione e sequestro, la presenza di personale in grado di rimuovere e maneggiare l'hard disk senza danneggiarlo e, soprattutto, in grado di verificare la presenza di dispositivi in grado di impedire l'accesso ai dati in esso contenuti.

In tal senso si è recentemente espressa la Corte di Cassazione[19] che, decidendo in merito al sequestro dell'intero computer (comprese periferiche varie), ha stabilito che, trattandosi di sequestro probatorio, la prova in ordine alla sussistenza del reato è tutelabile limitando il sequestro alla memoria fissa del computer e ad eventuali supporti contenenti elementi utili alle indagini ordinando, invece, la restituzione di tutti gli apparati "neutri" (stampanti, scanner, schede video...).

Vi sono, tuttavia, casi in cui è non solo consigliato, ma addirittura necessario procedere al sequestro dell'intero computer e delle relative periferiche. L'analisi dettagliata dell'intera casistica esula dalla portata del presente lavoro, ragion per cui ci si limiterà qui ad osservare come esemplare il caso delle indagini per divulgazione di materiale pedo pornografico.

In tale frangente il sequestro si rende necessario, non soltanto ai sensi dell'articolo 253 (sequestro probatorio), ma ai sensi dell'articolo 321 (sequestro preventivo), in quanto trattasi di beni di cui vi è obbligo di confisca[20]. Allo stesso modo la materiale disponibilità di beni informatici, soprattutto nei casi più gravi di divulgazione, rende possibile per l'imputato protrarre o aggravare le conseguenze del reato[21].

Proprio in merito all'acquisizione si ha il principale confronto tra differenti correnti dottrinarie: una prima che vede nell'analisi un accertamento irripetibile ed

[19] Cass. sez. III, sentenza 18/11/2003, n. 1778.
[20] Art.600 *septies* c.p.
[21] In tal senso Cass. sez. III, 10 febbraio 2005, n. 10058. Conforme Cass. pen., sez. V, 19 marzo 2002, n. 2816 in cui la Corte stabilisce che "*è legittimo il sequestro di un server informatico (completamente sigillato) presso lo studio di un avvocato indagato di concorso in bancarotta fraudolenta, al fine di verificare, con le garanzie del contraddittorio anticipato, la natura effettivamente pertinenziale rispetto al reato ipotizzato, di atti e documenti sequestrati, così escludendo indebite conseguenze sulle garanzie del difensore in violazione dell'art. 103 c.p.p. (Nella fattispecie la Corte ha ritenuto che il sequestro era funzionale alla selezione dei dati informatici pertinenti attraverso l'incombente processuale della perizia da espletarsi con incidente probatorio)*.".

una seconda che, invece, lo considera ripetibile.

La differenza non è soltanto terminologica, ma ha pesanti ricadute in sede processuale: l'accertamento ripetibile, infatti, può essere compiuto senza dare alcuna comunicazione alle parti, ma, di contro, la difesa potrà sempre richiedere, in sede dibattimentale, che questo venga ripetuto alla presenza delle parti e di un perito, nominato dal Giudice.

L'accertamento non ripetibile, invece, parte dal presupposto che la cosa sia soggetta a modifica e prevede che il PM dia avviso alla persona offesa ed alla persona sottoposta alle indagini del luogo, del giorno e dell'ora previsti per il conferimento dell'incarico, affinché questi possano partecipare con propri consulenti. Prima dell'inizio delle operazioni l'indagato può formulare riserva di incidente probatorio e, in tal caso, si procederà alle operazioni in tale sede.

Non vi è dubbio che tale pratica sembri offrire le maggiori garanzie difensive, ma vi sono almeno due elementi che bisogna tenere in considerazione: in primo luogo si tratta di un accertamento tecnicamente ripetibile (salvo grossolani errori del consulente oppure circostanze particolari), quindi non è tecnicamente possibile parlare di accertamento non ripetibile; in secondo luogo l'utilizzo di un simile strumento, laddove si proceda nei confronti di ignoti, rappresenterebbe una grave lesione al diritto alla difesa per il soggetto che, successivamente iscritto nel registro degli indagati, non soltanto non avrebbe alcuna possibilità di ottenere una nuova analisi del supporto in sede di dibattimento, ma ben potrebbe trovarsi di fronte ad un reperto ormai alterato; la valutazione dell'accertamento come non ripetibile, infatti, consentirebbe di effettuare anche operazioni in grado di provocare modifiche (per esempio l'avvio della macchina da analizzare senza alcuna cautela).

Proprio per tali ragioni, è indubbiamente preferibile procedere, ogni qualvolta ciò sia possibile, con la formula dell'accertamento ripetibile, fermo restando il fatto che, in presenza di errori o attività che apportino modifiche alla struttura del reperto, lo stesso dovrebbe essere considerato "inquinato" e le risultanze in esso contenute non più genuine né utilizzabili in dibattimento. Dunque, per garantire la ripetibilità dell'analisi (vero principio cardine della *computer forensics)*[22], è

[22] Sul punto la dottrina in materia di *computer forensic* è decisamente categorica. Si veda, *infra multis, G. Costabile, Scena criminis, cit.*; AA.VV., *Electronic Crime Scene Investigation: a guide*

necessario operare sempre su di una copia del supporto sequestrato; naturalmente non è sufficiente un semplice ghost del disco rigido, ma è necessario che si tratti di una perfetta duplicazione (tanto che in gergo si parla spesso di "clonare" un hard disk) che, a differenza della mera copia, consentirà di operare su un hard disk praticamente identico all'originale, consentendo, quindi, l'analisi anche di eventuali aree apparentemente vuote[23].

In commercio esistono numerosi prodotti, hardware e software, in grado di "clonare" un hard disk, garantendo la non alterazione dell'originale e l'esatta corrispondenza originale-copia. Si può trattare di prodotti software commerciali (Encase, ForensicToolkit), open source (dd, aimage, dcfldd, AFF) oppure di apparecchi *hardware* (*hardcopy*, *diskjokey*, i vari prodotti Logicube). Più economici i prodotti software (soprattutto quelli *open source*), più sicuri gli apparecchi *hardware,* ormai realizzare una copia, garantendo la ripetibilità dell'accertamento, non dovrebbe più rappresentare un problema[24].

---

for first responders, *cit.*; E. CASEY, *Digital Evidence and Computer Crimes*, London, 2004; D.L. SHINDER, *Scene of the Cybercrime Computer Forensics Handbook,* Syngress, 2002; R. CLIFFORD, *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime*, Durham, 2001.

[23] Cfr M. MARTUCCI, *I Crimini ad Alta Tecnologia e l'Arma dei Carabinieri*, in marcomattiucci.it; B. FIAMMELLA, *Problematiche giuridiche in tema di computer forensic, cit.*

[24] In tal senso si veda: Cass. pen., sez. un., 24 aprile 2008, n. 18253; Cass. pen., sez. I, 25 febbraio 2009, n. 11503 "*Non dà luogo ad accertamento tecnico irripetibile la lettura dell'hard disk di un computer sequestrato, che è attività di polizia giudiziaria volta, anche con urgenza, all'assicurazione delle fonti di prova*. *Rigetta, Trib. lib. Napoli, 17 Ottobre 2008*"; Cass. pen., sez. III, 09 giugno 2009, n. 28524 "*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 durante il termine per comparire all'udienza dibattimentale senza contraddittorio e alla sola presenza del custode, in quanto implicano accertamenti ed interventi di persone qualificate e l'utilizzo di appositi strumenti, sì che devono essere necessariamente svolti in dibattimento, nel contraddittorio, e sotto la direzione del giudice. Rigetta, App. Bolzano, 03 aprile 2008*". Si veda, poi, Cass.Pen, sez.I, 18 febbraio 2009, n. 25191 secondo cui "*Ed invero la giurisprudenza di questa Corte è univoca nel ritenere che le attività di estrazione di copia di file da computer sottoposti a sequestro è da ricondurre alla fattispecie prevista dall'art. 258 c.p.p.. E' questa, in particolare, la soluzione accolta da Cass. sez. Un. sent. 24 aprile 2008, n. 18253, Tchmil, rv. 239397, con riferimento ad ipotesi nelle quali era stata disposta la restituzione di computer precedentemente sequestrati, previa estrazione di copia di alcuni file ritenuti utili ai fini delle indagini. Le Sezioni Unite, in particolare, hanno specificato che il relativo provvedimento di acquisizione di copia, disciplinato dall'art. 258 c.p.p., è autonomo rispetto al decreto di sequestro, e non è soggetto ad alcuna forma di gravame, stante il principio di tassatività delle impugnazioni*.

La nozione di accertamento tecnico non ripetibile, del resto, si basa sulla sussistenza di almeno due requisiti: a) deve trattarsi di una attività di carattere valutativo su base tecnico - scientifica, e non di una attività di constatazione, raccolta o prelievo dei dati materiali pertinenti al reato; b) tale attività deve avere ad oggetto persone, cose o luoghi soggetti a modificazioni tali da far perdere loro, in tempi brevi ogni valenza, probatoria in relazione ai fatti su cui vertono le indagini.

Orbene nessuno dei predetti requisiti risulta sussistere nel caso in esame, in quanto, anche ove si ritenga dimostrata la presenza di effettivi rischi di alterazione dei dati (e non di una astratta eventualità del genere), resta comunque difficile ricondurre l'attività di estrazione di co-

Da ultimo, è sempre buona norma procedere all'acquisizione della firma elettronica dell'intero supporto acquisito, con un'operazione detta "hashing". L'operazione viene tipicamente compiuta utilizzando un algoritmo MD5, che, generando un'impronta della lunghezza di 128 bit (16 byte), costituisce un riferimento certo alla traccia originale, pur non consentendone la ricostruzione[25]. Sebbene la compromissione dell'algoritmo MD5 sia, ad oggi, possibile soltanto teoricamente, soprattutto per dati della dimensione di un moderno had disk, sempre più spesso si ricorre ad un algoritmo della famiglia SHA[26].

Se si rende necessario avviare il computer, ad esempio nel corso di un'ispezione o per effettuare un'analisi preliminare, è necessario proteggere l'hard disk con un dispositivo che inibisca la scrittura sullo stesso (*write blocker*), a tal fine è consigliabile utilizzare un apparato hardware, in modo da effettuare una copia precisa dell'hard disk che consenta di avviare la macchina utilizzando un hard disk uguale all'origine, conservando quest'ultimo in un luogo sicuro.

Decisamente più valida è, però, l'ulteriore alternativa di realizzare una macchina virtuale, per esempio utilizzando VmWare o Virtual Box, in grado di consentire di avviare la macchina in modalità soltanto virtuale, senza apportare alcuna modifica ai dati in essa contenuti.

In merito a quest'ultimo punto, si consideri che numerosi software di crittografia o di steganografia consentono di impostare un meccanismo di protezione che danneggia il file protetto in caso di errori nell'inserimento della password (oppure inserendo un'apposita password), quindi, errori di digitazione in sede di ispezione potrebbero portare alla cancellazione delle tracce del reato.

Allo stesso modo un floppy, un CD, ma anche una periferica interna, se lasciati inseriti, potrebbero avviare una procedura di cancellazione dell'intero hard disk; in breve, l'avvio del sistema con il disco originale installato e collegato è

---

pia dei file nell'alveo delle attività di carattere valutativo su base tecnico – scientifica".

[25] Si osserva che tale algoritmo è utilizzato a livello internazionale e garantisce un buon livello di sicurezza anche se, recentemente, alcuni ricercatori cinesi hanno trovato una collisione dell'algoritmo.

[26] La sigla SHA rappresenta l'acronimo di *Secure Hash Algorithm,* una famiglia di cinque diverse funzioni crittografiche sviluppate dalla National Security Agency (NSA) e pubblicate dal NIST come standard federale dal governo degli USA. Gli algoritmi sono denominati SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512: il primo produce un *digest* del messaggio di 160 bit, mentre gli altri producono digest di lunghezza in bit pari al numero indicato nella loro sigla (i.e. SHA-256 produce un digest di 256 bit).

decisamente sconsigliato!

6. L'analisi dei reperti informatici rappresenta il culmine dell'attività investigativa, soprattutto di quella finalizzata alla repressione dei reati informatici, ma, per quanto apparentemente semplice, questa fase dell'indagine richiede una notevole attenzione e competenza: eventuali errori commessi in questa sede, potrebbero compromettere l'intera indagine, soprattutto in relazione alla successiva utilizzabilità processuale delle prove raccolte.

Non sempre le prove sono immediatamente individuabili, essendo ben possibile che le stesse siano dissimulate all'interno di altri files (steganografia), protette da meccanismi di crittografia o conservate all'interno di uno o più client di posta elettronica o *newsgroup*.

L'analisi dell'*hard disk*, ad esempio, rappresenta spesso la prova del nove nel corso di un'indagine per pedopornografia: non importa quali e quante prove si siano raccolte nelle precedenti fasi investigative, molto spesso l'analisi dell'*hard disk* è necessaria per dimostrare che il materiale è stato consapevolmente acquisito e, eventualmente, consapevolmente ceduto a terzi; proprio per tale ragione non è sufficiente verificare la mera presenza di immagini o filmati, ma bisogna dimostrare che il materiale è stato consapevolmente e volontariamente trattato.

Deve poi considerarsi che è oggi facile reperire programmi che consentono di creare un'intera partizione *fat32*, o *ntfs*, criptata; in alcuni casi, la partizione può comprendere l'intero sistema operativo con i relativi file (di *boot*, di *swap*, temporanei, etc.) ed è persino possibile che tale partizione si possa avviare solo utilizzando un apposito dischetto di *boot*; in assenza del *floppy* la partizione appare come spazio non formattato.

In relazione a crittografia e steganografia, è bene ricordare che si tratta di programmi perfettamente legittimi il cui utilizzo, in assenza di ulteriori elementi a carico, non può essere valutato a sfavore dell'imputato. Tra l'altro è opportuno ricordare che, secondo la legge italiana, l'imputato ha il pieno diritto di rifiutarsi di consegnare le eventuali password, anche se necessarie ad accedere a file e/o cartelle crittografate; tale comportamento può, tuttavia, essere valutato negativamente dal Giudice nel caso di un'eventuale condanna.

Una volta effettuata la copia dell'*hard disk*, è possibile procedere all'analisi del suo contenuto avendo cura che anche le operazioni compiute in questa fase siano dettagliatamente documentate e, soprattutto, ripetibili. A tal proposito, parte della dottrina americana[27], ha contestato l'utilizzo di software proprietari per eseguire l'analisi e generare un rapporto: in linea di massima si sostiene che quando ci si avvale di tali programmi non è possibile sapere come si è arrivati ad un determinato risultato (per esempio recupero di una cartella cancellata)[28].

Tuttavia, laddove l'accertamento sia ripetibile, la questione è facilmente risolvibile: la possibilità di ripetere l'esame in sede di dibattimento è di per sé idonea garanzia del rispetto del diritto di difesa dell'imputato. In realtà, il corretto interrogativo dovrebbe essere non tanto che *tool* è stato utilizzato, ma se l'analista aveva o meno il necessario background tecnico e legale[29].

Ciò che, in realtà, veramente conta è, infatti, la preparazione e lo scrupolo del soggetto che fisicamente esegue l'analisi; si prenda, ad esempio, un'indagine in tema di detenzione di materiale pedopornografico: l'approccio più corretto porta a richiedere, spesso sin dalle fase delle indagini preliminari, non soltanto di valutare la presenza di materiale, ma anche di escludere (o confermare!) che la detenzione dello stesso sia avvenuta inconsapevolmente, ad esempio perché si è erroneamente scaricato un filmato pedo pornografico dai circuiti del p2p, ovvero si è involontariamente acceduto ad un sito pedo pornografico[30].

---

[27] Cfr B. Carrier, *Open Source Digital Forensics Tools, The Legal Argument*, in http://www.digital-evidence.org. Si veda anche A. Monti, *Attendibilità dei sistemi di computer forensic*, in http://www.ictlex.net

[28] Per un dettagliato documento relativo alle metodologie di analisi dei *software* destinati alla *computer forensics* si veda AA.VV., *General Test Methodology for Computer Forensic Tools*, November 7, 2001, National Institute of Standards and Technology, U.S. Department of Commerce. Si veda anche AA.VV., *CYBER-FORENSIC RESEARCH EXPERIMENTATION AND TEST ENVIRONMENT (CREATE)*.

[29] In tal senso si veda S. Hailey, *The "Tools Proven In Court" Question,* in http://www.cybersecurityinstitute.biz secondo cui la prima domanda dovrebbe essere non tanto che tool è stato utilizzato, ma "*does the analyst have the technical background to support the results of their investigation, have they properly authenticated their results, and was a sound investigation performed from start to finish?*".

[30] In tal senso si veda Tribunale di Perugia, 8 luglio 2003, n.313/03 in cui il GUP osserva "*Quanto alle immagini estratte dalla Polizia Postale dalla memoria del disco fisso del pc del Tizio, deve invece condividersi l'assunto della difesa: non è adeguatamente provato che l'imputato fosse un utente di internet così evoluto da sapere che ogni immagine, sia pure visualizzata per un tempo minimo sul monitor, rimane immagazzinata nella cartella dei cosiddetti files temporanei. Quella cartella, in vero, non risponde a finalità di archivio in senso stretto, ma ha l'unica finalità di rendere più rapido l'accesso ad un sito (e ad un documento) già visionato, ove si decida di accedervi di nuovo: si tratta dunque di una sorta di memoria invisibile del computer, che solo persone di particolare abilità e con strumenti tecnici adeguati sono in grado di riportare alla luce, a diffe-*

Proprio per tale ragione, perplessità sorgono in merito all'utilizzabilità di file cancellati e recuperati dal disco rigido senza alcuna indicazione dell'originaria collocazione, laddove la detenzione consapevole dei suddetti file non venga in qualche modo confermata da elementi esterni, per esempio tracce delle ricerche effettuate utilizzando un motore di ricerca.

7. Al termine di questo breve esame, occorre spendere due parole in merito alla possibilità che l'analisi di evidenze informatiche debba essere eseguita nel corso di un procedimento civile. In tali casi è assolutamente necessario che consulenti e perito circoscrivano l'ambito e la tipologia dei file da esaminare.

In sede civile, infatti, si contrappongono due parti private e, pertanto, decisamente maggiore rispetto alla sede penale è il rischio di una violazione della riservatezza dei dati custoditi nel computer[31] e, soprattutto, di un loro illecito

---

renza della c.d. "cronologia" dei siti visitati.

Anche utenti medi di internet sanno, ma comunque non è provato che il Tizio lo sapesse, che ogni programma di navigazione in rete (Netscape, Internet Explorer, ecc.) prevede una "cronologia" dei documenti scaricati sul video, sia pure non archiviati o salvati su disco: per alcuni giorni, con un periodo di conservazione che l'utente può impostare a sua scelta, quei documenti rimangono di pronto accesso, e sono visibili anche in modalità "non in linea", cioè a prescindere da una nuova navigazione. In quel caso, e fino alla scadenza del termine impostato, vi è perciò una vera e propria forma di detenzione di quel materiale (ovviamente, su supporto informatico, non essendone necessaria la stampa su carta), perché conservato e immediatamente fruibile: ma non altrettanto accade con la cartella dei temporary internet files, con l'utente che non può normalmente riaccedere a quei dati ed il più delle volte neppure sa di averne conservato traccia.

In definitiva, è certo che il Tizio visitò i siti da cui trasse le 22 immagini indicate al capo B), immagini che vide riprodotte sul suo schermo; è altrettanto certo che non ne fece una copia da archiviare nelle normali cartelle del disco fisso. E' possibile che per qualche tempo le foto in questione rimasero nella "cronologia" del pc, ma può anche darsi che l'imputato non avesse impostato affatto termini di conservazione, e così pure che non fosse consapevole di quella modalità di archiviazione automatica e temporanea; non è comunque provato che sospettasse l'esistenza dei files temporanei di internet"; in tal senso si veda anche Trib. Brescia, 24/05/2004, "*Elementi costitutivi del reato di cui all'articolo 600 quater del c.p. sono, sul piano obiettivo, la detenzione di materiale avente l'indicato contenuto; sul piano soggettivo, la consapevolezza - non solo, ciò che è sin troppo ovvio, della detenzione del materiale, ma, soprattutto - della natura illecita, e in specifico afferente allo sfruttamento di minori, del materiale stesso. Con riferimento ai materiali informatici, e, segnatamente, a quelli connessi a navigazione nel web, va rilevato che la norma, punendo chi "si procura o dispone" di materiale illecito, e non chi, semplicemente, lo visiona, consente lo svolgimento della pretesa punitiva non nei confronti di tutti coloro che, navigando in internet, "entrino in contatto", semplicemente, con immagini aventi quel contenuto, ma coloro che "se ne approprino", salvandole e veicolandole o sul disco fisso del Pc o su altri supporti, con esso interfacciabili, che ne consentano la visione o comunque la riproduzione. Lo scaricamento dei materiali, ovviamente, deve essere consapevole e volontario, dovendosi escludere profili di responsabilità penale nei casi in cui il materiale rinvenuto sul Pc costituisca la mera traccia di una trascorsa consultazione del web, creata dai sistemi di salvataggio automatico del personal computer*".

[31] In tal senso si veda il caso n°4:05-cv-00328-RAS, *Sony BMG Music Entertainment Vs Kim Arellanes* in cui la convenuta si è rifiutata di consegnare all'attore (BMG) il proprio *hard disk* sostenendo la necessità che l'analisi sia condotta da un esperto indipendente anche, e soprattutto, a garanzia

utilizzo ad opera della controparte.

In tale sede, l'analisi preliminare del supporto dovrebbe essere condotta da parte del CTU: ai CTP dovrebbe poi essere consentito accedere esclusivamente ai dati relativi al procedimento in corso, senza poter in alcun modo visionare eventuali altri dati personali, estranei al procedimento e contenuti nell'*hard disk*.

Tuttavia non sempre, nella pratica quotidiana, è possibile seguire questa prassi; si pensi alla fattispecie tipica della contestazione ad un dipendente di attività di concorrenza sleale o di utilizzo improprio degli strumenti informatici messi a disposizione dal proprio datore di lavoro.

In tutte queste circostanze, sarà necessario fare riferimento alle linee guida del Garante in materia di posta elettronica e internet[32], in modo da operare nel pieno rispetto della tutela della riservatezza del lavoratore, pur riconoscendo il giusto diritto del datore di lavoro ad assicurare la funzionalità e il corretto impiego dei mezzi informatici da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa.

Non può, infatti, sfuggire che l'utilizzo di Internet da parte dei lavoratori può formare oggetto di analisi, profilazione e integrale ricostruzione della navigazione web grazie ai dati ottenuti, ad esempio, da server aziendale o da un altro strumento di registrazione delle informazioni e che le informazioni così trattate contengono dati personali, ma anche dati sensibili, riguardanti lavoratori o terzi, identificati o identificabili. Per tale ragione, l'attività di analisi e di valutazione dei supporti informatici aziendali in vista di un procedimento civile dovrà essere effettuata avendo ben chiari i principi di pertinenza e non eccedenza.

In base a tali principi, l'analisi potrà essere effettuata soltanto laddove effettivamente necessaria, riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite[33]; i lavoratori dovranno essere stati preventivamente informati della possibilità di controlli a posteriori,

---

dei file personali della convenuta (e-mail, fotografie, messaggi personali...) estranei alla vicenda. L'attore si è opposto alle richieste del convenuto sostenendo che soltanto l'analisi del supporto da parte di un proprio esperto di fiducia avrebbe garantito il pieno rispetto dell'attore all'acquisizione di prove a sé favorevoli. Il Giudice Richard A. Schell accoglieva le eccezioni della convenuta, disponendo che l'analisi fosse effettuata da un perito neutrale.

[32] Garante per la protezione dei dati personali, Deliberazione 01 marzo 2007 in Bollettino n. 81 del marzo 2007, "*Lavoro: le linee guida del Garante per posta elettronica e internet*" in Gazz.Uff., n. 58 del 10 marzo 2007.

[33] Principio di necessità.

che determinino trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa[34]; gli ulteriori trattamenti dovranno essere effettuati per finalità determinate, esplicite e legittime, osservando il principio di pertinenza e non eccedenza. In ogni caso, i dati dovranno essere trattati "*nella misura meno invasiva possibile*" e le attività di analisi dovranno essere "*mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza*"[35].

E' molto importante ribadire che all'onere del datore di lavoro di prefigurare e pubblicizzare una policy interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice: i dipendenti hanno, infatti, il diritto di essere informati, preventivamente ed in modo chiaro, sui trattamenti di dati che possono riguardarli.

8. Particolare attenzione viene posta dal Garante a proposito delle apparecchiature preordinate al controllo a distanza dei lavoratori.

Si osserva, infatti, che il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro, ma, nell'esercizio di tale prerogativa, occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare "*apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori*".

In caso di installazione il loro utilizzo determina un illecito trattamento dei dati, a prescindere dall'illiceità dell'installazione stessa ed anche laddove i singoli lavoratori ne siano consapevoli[36]; in particolare, il Garante ha stabilito che non

[34] Principio di correttezza.

[35] In tal senso si veda il Parere 8/2001 sul trattamento di dati personali nell'ambito dei rapporti di lavoro adottato il 13 settembre 2001.

[36] Cass. civ., sez. lav., 18 febbraio 1983, n. 1236, in *Foro it. 1985, 2076* "*L'installazione in azienda, da parte del datore di lavoro, di impianti ed apparecchiature richiesti da esigenze produttive, dai quali derivi anche una mera possibilità di controllo a distanza sull'attività lavorativa dei dipendenti, deve essere preceduta da un vero e proprio accordo con le rappresentanze sindacali aziendali, non essendo sufficiente a legittimare l'installazione nè il fatto che le maestranze fossero a conoscenza dell'esistenza degli impianti potenzialmente idonei al controllo nè la circostanza che gli impianti stessi abbiano funzionato per un determinato periodo di tempo senza contestazioni da parte dei lavoratori (nella specie sono stati individuati come strumenti di controllo "preterintenzionale" a distanza dell'attività dei lavoratori, soggetti alla disciplina dell'art. 4, comma 2 l. n. 300 del 1970, dei dischi - installati dagli stessi dipendenti sulle macchine di lavorazione all'inizio*

può ritenersi consentito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire – a volte anche minuziosamente – l'attività di lavoratori[37]. Il controllo a distanza riguarda tanto l'attività lavorativa in senso stretto che le altre condotte personali poste in essere nel luogo di lavoro, pertanto, pur prescindendo da eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili in alcun modo[38].

In relazione ai programmi che consentono controlli "indiretti" (c.d. controllo preterintenzionale), il Garante osserva che il trattamento di dati che ne consegue può risultare lecito, purché siano rispettate le procedure di informazione e di consultazione di lavoratori e sindacati, in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici, destinati a

---

della loro prestazione e collegati ad un registratore Kienzle - sui quali restano impressi tracciati grafici differenti a seconda delle diverse fasi di funzionamento o di arresto automatico della macchina, tracciati che consentono di valutare "a posteriori" l'efficienza degli operai, la tempestività dei loro interventi minuto per minuto, le pause eccessive di lavoro)" e Cass. civ., sez. lav., 16 settembre 1997, n. 9211, in *Giust. civ. Mass. 1997, 1727*, "*L'installazione in azienda, da parte del datore di lavoro, di impianti audiovisivi - che è assoggettata ai limiti previsti dall'art. 4 stat. lav. anche se da essi derivi solo una mera potenzialità di controllo a distanza sull'attività lavorativa dei dipendenti, senza che peraltro rilevi il fatto che i dipendenti siano a conoscenza dell'esistenza di tali impianti - deve essere preceduta dall'accordo con le rappresentanze sindacali aziendali, non essendo sufficiente, in ragione della tassatività dei soggetti indicati dal comma 2 dell'art. 4 cit., a legittimare tale installazione un'intesa raggiunta dal datore di lavoro con organi di coordinamento delle r.s.a. di varie unità produttive; con l'ulteriore conseguenza che è identificabile in tale fattispecie un comportamento antisindacale del datore di lavoro, reprimibile con la speciale tutela approntata dall'art. 28 stat. lav., la quale prescinde dall'esistenza di alcuno specifico elemento intenzionale*".

[37] Il Garante fa esplicito riferimento ai seguenti esempi:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- analisi occulta di computer portatili affidati in uso.

[38] Si veda l'art. 11, comma 2, del Codice per la protezione dei dati personali. Si veda anche Cass. civ., sez. lav., 17 giugno 2000, n. 8250, in *Giust. civ. Mass*., 2000, 1327, "*L'uso di una telecamera a circuito chiuso, finalizzata a controllare a distanza anche l'attività dei dipendenti, è illegittimo ai sensi dell'art. 4 della l. n. 300 del 1970; ne consegue, sul piano processuale, che non può attribuirsi alcun valore probatorio al fotogramma illegittimamente conseguito. (Nella specie, la sentenza di merito, confermata dalla S.C., aveva respinto la domanda proposta da una società proprietaria di un pubblico esercizio nei confronti di una dipendente, intesa al risarcimento dei danni derivanti dalla sottrazione di somme custodite nella cassa e fondata sulla produzione di fotogramma proveniente da una telecamera a circuito chiuso installata nell'esercizio ove la dipendente prestava lavoro)*".

controllare i movimenti o la produttività dei lavoratori.

Prescindendo, qui, dall'indicazione del Garante di privilegiare, rispetto all'adozione di misure "repressive", ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri, si osserva come la mancata esplicitazione di una precisa policy al riguardo dell'utilizzo degli strumenti informatici, può determinare una legittima aspettativa del lavoratore, o di terzi, sulla confidenzialità di tali forme di comunicazione, che si riverbera sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro, che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore o di quelli inviati da quest'ultimo.

In tutti questi casi, l'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza; per esempio, nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

In ogni caso, deve, per quanto possibile, essere privilegiato un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa ovvero a sue aree, svolto in forma anonima e che può concludersi con un avviso generalizzato, relativo ad un rilevato utilizzo anomalo degli strumenti aziendali, seguito dall'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Laddove l'avviso non sia seguito da ulteriori anomalie, effettuare ulteriori controlli su base individuale non è, di regola, giustificato. Del pari viene esclusa l'ammissibilità di controlli prolungati[39], costanti o indiscriminati.

In ogni caso, il trattamento dei dati personali dovrà essere limitato alle sole informazioni indispensabili per perseguire quelle finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Nel caso di datori di lavoro privati e di enti pubblici economici, il trattamento può essere legittimamente effettuato soltanto:

[39] L'eventuale prolungamento dei tempi di conservazione deve essere valutato come eccezionale e trova giustificazione soltanto laddove sia legato ad esigenze tecniche o di sicurezza del tutto particolari, all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria ed all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria[40];

b) in caso di valida manifestazione di un libero consenso;

c) in presenza di un legittimo interesse al trattamento in applicazione della disciplina sul cosiddetto bilanciamento di interessi[41].

L'accesso del consulente sarà, quindi, lecito e possibile soltanto laddove il lavoratore sia stato preventivamente informato della possibilità di controlli ed il controllo stesso sia pertinente e non eccedente rispetto alle esigenze di tutela degli interessi del datore di lavoro.

[40] Cfr. art. 24, comma 1, lett. f) del Codice.
[41] Cfr. art. 24, comma 1, lett. g), del Codice.