

# **Protezione delle informazioni. Privacy e sicurezza.**

A cura di : Fabio Di Resta

***(Estratti dei Capitoli V e XI)***

—

Estratto del Cap. V

**“TUTELA DELLA PRIVACY NEL RAPPORTO  
DI LAVORO: CONTROLLO A DISTANZA DEL LAVORATORE  
E TELELAVORO “**

*(da pag. 151 a pag. 158)*

Autore : Fabio Di Resta.

—

Estratto del Cap. XI

**“SICUREZZA INFORMATICA ED  
ACQUISIZIONE DELLE PROVE “**

*(da pag.336 a pag. 339)*

Autori : Massimino Boccardi,  
e Gianfranco Gargiulo.



**G. Giappichelli Editore**

**Finito di stampare a Novembre 2008**

300/1970, riferito esclusivamente all'uso di apparecchiature di controllo a distanza (non applicabile analogicamente, siccome penalmente sanzionato)»

Cass., Sez. lav., 12 giugno 2002, n. 8388, in *Mass. Giust. civ.*, 2002, 1000; conf. Cass., Sez. lav., 9 giugno 1990, n. 5599, in *Riv. giur. lav.*, 1990, II, p. 453.

In un caso relativo ad un supposto licenziamento per ritorsione<sup>5</sup> nel quale un dipendente aveva installato dei registratori in azienda per il rilevamento sia di conversazioni con i superiori gerarchici, con colleghi e datore di lavoro, la Cassazione nel confermare il potere di direzione e gerarchia dell'imprenditore ha poi escluso l'applicazione del comma 2 dell'art. 4 S.d.L. (c.d. controlli preterintenzionali) alla fattispecie, poiché l'ambito soggettivo della norma era rivolto al solo datore di lavoro e non ad altri soggetti,

Giurisprudenza 

«la suddetta disposizione, con il consentire, come detto, al solo datore di lavoro i controlli sui lavoratori, attesta che il legislatore ha inteso vietare ogni forma di controllo (occulto o palese) effettuato con modalità diverse da quelle da esso indicate ed ad opera di soggetti diversi dal datore di lavoro o dal personale addetto alla vigilanza (cfr.: art. 3 S.d.L.). L'assolutezza del divieto, che accompagna la previsione legislativa, si giustifica in ragione del rispetto della "personalità" del lavoratore e della sua dignità, che impongono che non siano annullati quei margini di riservatezza nella "vita aziendale" che ogni lavoratore ha diritto a vedere osservati»

Cass. Civ., Sez. lav., 3 maggio 1997, n. 3837, *Scopece c. Soc. Italgas*, in *Mass. Giust. civ.*, 1997).

### 3. *Esigenza di bilanciare gli opposti interessi tra la tutela del patrimonio aziendale e la privacy del lavoratore*

Nel Codice della Privacy, il Capo III della disciplina relativa al lavoro e previdenza sociale titola divieto di controllo a distanza e telelavoro, si compone di due articoli, artt. 114 e 115 C.d.P. Il primo articolo rinvia integralmente all'art. 4 S.d.L., il quale al comma 1 dispone il divieto dell'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a di-

---

<sup>5</sup> Il licenziamento per ritorsione viene inteso come il licenziamento attuato in seguito di comportamenti sgraditi all'imprenditore. Nella sentenza in esame l'aspetto ritorsivo del licenziamento viene escluso in quanto non era stato dimostrato l'intento «vendicativo», questo non essendo provato per il solo fatto del riferimento alla causa di lavoro precedentemente instaurata con il datore di lavoro.

stanza dell'attività dei lavoratori. Si tratta di un divieto posto a tutela della riservatezza sul luogo di lavoro (*rectius* riservatezza dei dati personali del lavoratore), sotto un profilo oggettivo la norma richiama sia gli impianti audiovisivi, quindi dispositivi volti ad immagazzinare sia immagini che suoni, ovvero anche soltanto gli uni (immagini esclusivamente video) o soltanto gli altri (registrazioni sonore), l'inciso «altre apparecchiature» invece viene comunemente ritenuto come un termine volutamente più generico e idoneo a includere una moltitudine non precisata di apparecchi capaci di svolgere la funzione di controllo a distanza. Così in dottrina è stato affermato con riferimento all'inciso in esame «*apparecchiatura di controllo è qualsiasi congegno o parte di congegno dotato di potenzialità o suscettibile di essere usato in funzione di controllo, ovunque collocato ed inserito, e non necessariamente caratterizzato da una sua distinta e autonoma struttura o da un'esclusiva destinazione al controllo*»<sup>6</sup>. Si ritiene che anche la giurisprudenza di legittimità accolga un'ampia definizione di impianti o apparecchiature e consente perciò una interpretazione estensiva dell'inciso in esame,

Giurisprudenza 

«l'interpretazione estensiva è consentita anche in materia di leggi penali: essa mira, infatti, a fare esattamente coincidere la norma con il pensiero e volontà del legislatore, essendo doveroso per l'interprete, [...] applicare la norma più ampiamente di quanto la dizione letterale comporterebbe»

Cass. Sez. III, 25 marzo 1963-7 maggio 1963, n. 894, in *Giur. pen.*, 64, I, p. 73.


«Pur non essendo suscettibile di applicazione analogica perché penalmente sanzionabile»

Cass., Sez. lav., 3 maggio 1997, n. 3837, in *Dir. prat. lav.*, 1997, 32, p. 2316).

Da una parte è perciò giusto rispettare i limiti posti a tutela della personalità del lavoratore e della sua dignità, i quali impongono che non siano annullati quei margini di riservatezza nella «vita aziendale» che ogni lavoratore ha diritto a vedere osservati, anzi vanta un «*diritto soggettivo a non essere sottoposto a controlli a distanza al di fuori delle ipotesi contemplate dalle legge*». Dall'altra, il fatto che la violazione dell'art. 4 S.d.L. sia assistita da sanzione penale *ex artt.* 38 S.d.L. e 171 C.d.P., vieta la sola interpretazione analogica, ossia regolamentazione di un caso non disciplinato né implicitamente né esplicitamente dalla legge che ha funzione integratrice del-

<sup>6</sup> A. ROSSI, *La libertà e la professionalità dei lavoratori di fronte alle nuove tecnologie informatiche*, in *Quest. giust.*, 1983, p. 220.

le norme giuridiche<sup>7</sup>. Ne deriva che il significato da attribuire all'inciso in esame comprenda ogni strumento elettronico con il quale si possa operare un controllo sia esso occulto, palese o di altro tipo, salve in ogni caso le esigenze aziendali specifiche tutelate dalla legge e le garanzie procedurali a diversi livelli prescritte dalla stessa.

Giurisprudenza 

«Con l'art. 4 S.d.L. il legislatore ha inteso evitare che con le innovazioni tecnologiche si introducesse in azienda un tipo di controllo che il lavoratore, anche consapevole, non percepisce immediatamente e al quale quindi è esposto in modo assillante, senza tregua e senza possibilità di difesa. La raccolta dei dati relativi a specifici eventi del rapporto di lavoro o il riepilogo degli stessi dati, effettuati, come nella specie, con l'ausilio di sistemi informatici ...»

Trib. Milano 29 settembre 1990, CUDA-AEM c. AEM, in *Notiziario giur. lav.*, 1990, p. 805.

Con questa ampia definizione di apparecchiature, l'elemento che caratterizza il dispositivo di controllo a distanza è quello funzionale riferito alla prestazione lavorativa, così rientrano nel controllo a distanza, gli impianti audiovisivi destinati all'uso e alla conservazione dei cartellini segna-orario.

Giurisprudenza 


«Il divieto posto dall'art. 4 S.d.L. per il datore di lavoro di far uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori non è escluso né dalla circostanza che tali apparecchiature siano state solo installate ma non siano ancora funzionanti, né dall'eventuale preavviso dato ai lavoratori, i quali quindi siano avvertiti del controllo suddetto, né infine del fatto che tale controllo sia destinato ad essere discontinuo perché esercitato in locali dove i lavoratori possono trovarsi solo saltuariamente»

Cass., Sez. lav., 6 marzo 1986, n. 1490, Società Italcementi c. FILCEA CISL e altro, in *Mass. giur. lav.*, 1986, p. 498.

Nel concetto di divieto di controllo a distanza ripreso dalla norma in esame, si ritiene in effetti che il riferimento alla distanza, sia da intendersi non con riferimento ad una dimensione fisica, ma al controllo occulto<sup>8</sup> effettuato soltanto tramite l'uso di apparecchiature, sono esclusi da tale definizione i controlli diretti a verificare comportamenti illeciti, in quanto comportamenti non attinenti alla prestazione lavorativa o alla diligenza in essa posta dal lavoratore.

<sup>7</sup> Cass., Sez. III, 21 maggio 1971-24 agosto 1971, n. 1136, *Cass. pen. Mass. annotato*, 72, p. 1236.

<sup>8</sup> G. AMOROSO-V. DI CERBO-A. MARESCA, *sub Art. 4*, in *Il diritto del lavoro*, Giuffrè, Milano, 2001, p. 31 ss.

Giurisprudenza 

«È legittimo il controllo occulto del datore di lavoro effettuato a mezzo di personale estraneo all'impresa e diretto a verificare la realizzazione di comportamenti che costituiscono, oltre che inadempimento contrattuale, illecito penale»

Cass., Sez. lav., 18 settembre 1995, n. 9836, Garenna c. Soc. Agape, in *Foro it.*, 1996, I, c. 609.

In tal senso, anche il Tribunale di Vibo Valentia ammette i controlli occulti volti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi),

Giurisprudenza 

«sono legittimi, e non violano gli artt. 2 e 3, legge 20 maggio 1970, n. 300, i controlli, anche occulti, diretti all'accertamento di comportamenti illeciti del lavoratore che esulano dalla normale attività lavorativa e che in tale attività trovano solo l'occasione»

Pret. Vibo Valentia 26 aprile 1991, Manco c. Società La Rinascente, in *Giur. merito*, 1991, p. 974, nota.

Il Tribunale di Rieti, ammette la legittimità di controlli occulti volti ad accertare la diligenza del prestare che anziché eseguire la prestazione lavorativa si dedichi ad attività extra-lavorative.

Giurisprudenza 

«Il divieto di controlli occulti sul lavoratore previsto dagli artt. 2 e 3, legge n. 300/1970 non opera laddove il datore di lavoro attivi detti controlli non già per verificare la diligenza del lavoratore nello svolgimento della sua attività ma la presenza o meno di una condotta fraudolenta da parte dello stesso il quale, simulando di uscire dal luogo di lavoro per recarsi, nell'ambito del proprio incarico aziendale, a trovare clienti e/o potenziali clienti, in realtà passi il tempo in tutte altre occupazioni estranee all'attività lavorativa»

Trib. Rieti 4 febbraio 1999, Petrongari c. Banca pop. Rieti, in *Orient. giur. lav.*, 1999, I, p. 20.

Dopo aver esaminato brevemente il comma 1 dell'art. 4, il quale come descritto contiene un divieto di effettuare i controlli a distanza diretti ovvero esclusivamente finalizzati sulla prestazione lavorativa, è opportuno analizzare il comma 2 dell'articolo in questione. Questo rientra nello spirito della *ratio* legislativa di tutela del patrimonio aziendale, in base a tale *ratio* si ammette la possibilità di effettuare controlli indiretti sui lavoratori, ponendo due limiti, uno sostanziale, riferito a specifiche esigenze aziendali, l'altro procedurale. Più in particolare, si ammette che qualora il datore di lavoro voglia installare impianti e altre apparecchiature di controllo che siano richiesti da esigenze organizzative, produttive, ovvero della sicurezza del lavoro<sup>9</sup>, dai quali


<sup>9</sup> Si ritiene che mentre la nozione di sicurezza sul lavoro ha un ambito di applicazione più

possa derivare la possibilità di controllo sull'attività dei lavoratori, debba pervenire ad un accordo con le rappresentanze sindacali aziendali, oppure commissioni interne. In difetto di accordo, su istanza del datore di lavoro si dispone con provvedimento dell'Ispettorato del lavoro<sup>10</sup>. Con riguardo alla costituzione delle rappresentanze l'art. 9 S.d.L. stabilisce i requisiti per costituire le rappresentanze sindacali aziendali.

Normativa 

«– Art. 19. *Costituzione delle rappresentanze sindacali aziendali.* – Rappresentanze sindacali aziendali possono essere costituite ad iniziativa dei lavoratori in ogni unità produttiva, nell'ambito delle associazioni sindacali, che siano firmatarie di contratti collettivi di lavoro applicati nell'unità produttiva. Nell'ambito di aziende con più unità produttive le rappresentanze sindacali possono istituire organi di coordinamento».

Peraltro, contro il provvedimento dell'Ispettorato è possibile proporre ricorso gerarchico al Ministero del lavoro e politiche sociali, in alternativa alla ricorso in sede giurisdizionale<sup>11</sup>.

Giurisprudenza 

«In realtà l'accertata tassatività dei soggetti indicati dal più volte citato art. 4, comma 2, non ammette che l'assenso possa essere manifestato da organismi sindacali diversi da quelli indicati dalla norma stessa»

Cass., Sez. lav., 16 settembre 1997, n. 9211.

Il controllo indiretto (c.d. controllo preterintenzionale), ricorre qualora le finalità per le quali gli apparecchi sono installati sono quelle di soddisfare le esigenze organizzative, produttive e di sicurezza del lavoro, per ricondurre le fattispecie concrete all'esigenze in esame è sempre necessaria un'analisi caso per caso, quando le finalità degli apparecchi installati rientrano in quelle prescritte saranno legittimi, mentre se cadono fuori costituiscono

---


delineato, il concetto di organizzazione e produttività abbiano significati molto più ampi e generici, i diversi contrasti giurisprudenziali in materia mostrano come questi concetti siano in effetti caratterizzati di confini labili e di difficile individuazione.

<sup>10</sup> Rinominato Direzione Provinciale del lavoro, Servizio Ispettivo.

<sup>11</sup> Il ricorso gerarchico ai sensi dell'art. 1, D.P.R. n. 1199/1971 è ammesso in unica istanza, ed il provvedimento emesso a seguito al primo ricorso è definitivo. Si ritiene da un lato, che il ricorso gerarchico sia uno strumento volto a garantire le censure di merito quando tale possibilità è preclusa nella sede giudiziaria, dall'altro lato l'unica istanza snellisce notevolmente i tempi per pervenire ad una decisione definitiva.

un controllo a distanza vietato dalla norma, il quale si traduce in un comportamento illecito del datore penalmente sanzionato<sup>12</sup>.


Con riferimento ai controlli finalizzati a sorvegliare lo svolgimento dell'attività lavorativa dei dipendenti ed in particolare ad accertare le condotte finalizzate ad illeciti da parte dei lavoratori, la Suprema Corte ha affermato che:

Giurisprudenza 

«Devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad es., i sistemi di controllo dell'accesso ad aule riservate o, come nella specie, gli apparecchi di rilevazione di telefonate ingiustificate»

Cass., Sez. lav., 3 aprile 2002, n. 4746, Società Sicurpol c. Pizzutelli, in *Notiziario giur. lav.*, 2002, p. 642.

Anche il Tribunale di Milano ammette la legittimità dei controlli difensivi:

Giurisprudenza 

«Il controllo a distanza dell'attività dei lavoratori cui si riferisce il divieto *ex art. 4*, legge n. 300/1970 è cosa diversa dall'utilizzo di strumenti cosiddetti di "controllo difensivo" tesi all'accertamento di eventuali condotte illecite da parte dei propri dipendenti ovvero, in caso di contestazioni da parte degli utenti, a provare la regolarità del servizio offerto dalla impresa»


Trib. Milano 5 luglio 2006, B. c. Soc. A.G, in *Orient. giur. lav.*, 2006, p. 3611.

La recente giurisprudenza ritiene che qualora in azienda si installi un controllo presenze tramite *badge* unito al controllo accessi, vi sia la necessità di un accordo con le rappresentanze sindacali ed in mancanza di questo dell'ottemperanza della garanzie procedurali previste dal comma 2 dell'art. 4 S.d.L. Con riferimento ai *badge* predisposti da un società al fine di agevolare i propri dipendenti muniti di autovettura, ad accedere al garage ove posteggiarla durante l'orario lavorativo, la stessa aveva anche installato un congegno di sicurezza volto a consentire l'ingresso a tale garage solo mediante un meccanismo elettronico attivato da un tesserino. Si consentiva in questo modo, mediante un meccanismo di sbarra di elevamento posto all'ingresso e all'uscita dal garage, la registrazione dell'identità del dipendente e l'orario del passaggio. Tramite l'incrocio di tali dati con quelli rilevati elet-

<sup>12</sup> Con la tecnica del rinvio l'art. 171 C.d.P. estende la contravvenzione *ex art. 38 S.d.L.*, il quale prevede da 15 giorni ad un anno di arresto, sia all'art. 113, comma 1 («*Annunci di lavoro e dati riguardanti prestatori di lavoro*») sia all'art. 114 C.d.P. («*Divieto di controllo a distanza*»).

tronicamente all'ingresso degli uffici, si poteva controllare il rispetto degli orari di entrata e uscita e presenza sul luogo di lavoro da parte dei dipendenti.


La Cassazione a questo riguardo si è così pronunciata statuendo che:

Giurisprudenza 

«Il riferimento all'attività lavorativa, oggetto della fattispecie astratta, non riguarda solo le modalità del suo svolgimento, ma anche il *quantum* della prestazione, il controllo sull'orario di lavoro, risolvendosi in un accertamento circa quantità di lavoro svolto, si inquadra, per ciò stesso, in una tipologia di accertamento pienamente rientrante nella fattispecie prevista dal richiamato art. 4, comma 2»

Cass., Sez. lav., 17 luglio 2007, n. 15892, Piluso c. Eni, in *Mass. Giust. civ.*, 2007, f. 7-8.


In tema di utilizzazione di un dispositivo di rilevamento presenze (*badge*) in azienda il Tribunale di Milano aveva affermato che:

Giurisprudenza 

«Il cartellino magnetico (*badge*) segna e cristallizza solo l'entrata e l'uscita nello e dallo stabilimento ma non è assimilabile al controllo a distanza del datore di lavoro»

Trib. Milano 26 marzo 1994, Soc. Sirti c. Faccini, in *Orient. giur. lav.*, 1994, p. 23.

In questo senso anche la Pretura di Napoli affermava:

Giurisprudenza 

«Il divieto di cui all'art. 4, legge n. 300/1970 postula l'uso di un'apparecchiatura esterna che operi automaticamente, senza l'intervento del lavoratore che si suppone controllato. (Nella specie, è stata ritenuta lecita l'installazione di un sistema di rilevazione delle presenze, perché tale sistema, da un lato riguarda dati del tutto estrinseci rispetto alla prestazione lavorativa, dall'altro, è attivato, di volta in volta, da ciascun dipendente mediante l'inserimento di un tesserino magnetico)»

Pret. Napoli 15 marzo 1990, FABI Napoli e altro c. Esattoria comunale Napoli e altro, in *Notiziario giur. lav.*, 1990, p. 226.

La Pretura di Milano con riguardo ai centralini telefonici affermava che:

Giurisprudenza 

«Si viola l'art. 4 nell'installazione – senza il preventivo accordo con le r.s.a. o con la commissione interna, oppure in subordine, senza le prescrizioni dell'ispettorato del lavoro – di un centralino telefonico automatico (Alcatel 2506/MI) atto a rilevare e a registrare, tramite una stampante, tutta una serie di dati, quali il numero dell'apparecchio interno chiamante, il numero


dell'utente esterno, la data, l'ora ed il minuto di inizio, la durata ed il numero degli scatti di ogni singola conversazione, e con possibilità di inclusione diretta in linea»

Pret. Milano 4 ottobre 1988, Rampezzotti e altro, in *Notiziario giur. lav.*, 1989, p. 436.

#### 4. Tutela dei lavoratori secondo la prassi decisoria del Garante privacy

##### 4.1. Controlli audiovisivi del datore e la riservatezza dei dipendenti

Per quanto attiene alla riservatezza dei dati personali trattati sul luogo di lavoro, il Garante si è pronunciato in numerosi casi, relativi a reclami, segnalazioni, ovvero a ricorsi<sup>13</sup> ex art. 7 C.d.P. L'attenzione dei cittadini su questo tema ha portato in particolare all'emanazione di due provvedimenti a carattere generale, ossia provvedimenti normativi applicabili ad una categoria di titolari del trattamento<sup>14</sup>. Si tratta del provvedimento generale del 29 aprile 2004 sulla videosorveglianza e del provvedimento generale del 1° marzo 2007, intitolato «*Linee guida del Garante per la posta elettronica e internet*». Il Garante in entrambi richiama prima di tutto i principi generali del trattamento, principio di finalità, di necessità, liceità e proporzionalità. Dei primi tre principi si è detto profusamente nella parte relativa alle regole sul trattamento dei dati personali ex art. 11, pertanto in questo paragrafo verrà sinteticamente illustrato solamente il principio di proporzionalità. Si tratta di un principio richiamato al fine di effettuare una valutazione di liceità del trattamento, sia in ordine alla scelta sul se e quali mezzi impiegare, sia sul come utilizzarli nella varie fasi del trattamento. In tal modo a proposito della videosorveglianza, il Garante ha affermato che:

Giurisprudenza 

«La videosorveglianza è, quindi, lecita solo se è rispettato il c.d. principio di proporzionalità, sia nella scelta se e quali apparecchiature di ripresa installare, sia nelle varie fasi del trattamento (art. 11, comma 1, lett. d) del Codice)»

provv. Garante 29 aprile 2004, in *Bollettino*, n. 49, aprile 2004.

<sup>13</sup> L'art. 141 C.d.P. disciplina le forme di tutela con le quali possono essere fatti valere i diritti garantiti dal Codice della Privacy, qualora l'interessato voglia far valere i suoi diritti ex art. 7, l'unica forma di tutela disponibile è il ricorso, per maggiori informazioni si rinvia alla parte sui diritti dell'interessato.

<sup>14</sup> I provvedimenti generali del Garante sono emanati sulla base dell'art. 154, lett. c), all'Autorità è consentito così di «prescrivere anche d'ufficio ai titolari del trattamento le opportune misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'art. 143».

### Fase 13 – *DISSEMINATION*

Questa fase consiste nella gestione delle informazioni ottenute dall'investigazione nel suo complesso e sulla loro possibile riusabilità per altri casi.

Ferma restando la validità degli altri modelli, è sicuramente da evidenziare che quello qui presentato disegna un processo complesso non focalizzato esclusivamente all'analisi della prova digitale, ma alla gestione di tutte le fasi che caratterizzano una indagine informatica in tutte le sue molteplici aree.

#### 10. *Le procedure di analisi delle evidenze digitali*

In questo paragrafo ci focalizzeremo sugli aspetti tecnico-operativi propri di un processo di investigazione digitale – fasi 6-7-8-9 del modello (*collection, transport, storage, examination*) –, ovvero sulla predisposizione di un piano di intervento ed analisi delle evidenze digitali. Tale piano dovrà includere una serie di procedure diversificate a seconda che si tratti di sistemi informatici attivi, *off-line* o disattivati. In particolare si intendono per sistemi «attivi», tutti quelli in linea, connessi alla rete dati e con tutti i servizi e le applicazioni configurate attive; per sistemi «*off-line*» tutti quelli che disconnessi dalla rete dati ma mantenuti con i servizi e le applicazioni attive, infine, per sistemi «disattivati» si intendono quei sistemi che sono disattivati e quindi non più operativi. Per tutti i casi sopraelencati le procedure di gestione delle evidenze digitali dovranno prevedere le modalità di acquisizione dello stato del sistema informatico in un determinato istante. Tale «fotografia» del sistema potrà consentire agli investigatori, dopo un'accurata analisi, di individuare gli elementi di prova ricercati.

Le modalità di acquisizione delle evidenze digitali riguardanti i sistemi oggetto di indagine variano in base allo stato del sistema analizzato. La tabella n. 2 illustra i dati che possono essere potenzialmente acquisiti dai sistemi in base al loro stato operativo:

	Sistema Attivo	Sistema Off-Line	Sistema Disattivato
Networking Data	✓	✓*	–
Volatile Data	✓	✓	–
Non-Volatile Data	✓	✓	✓
	* Dati parziali		
	Networking Data: <i>Sessions, traffic, arp table, ...</i>		
	Volatile Data: <i>ram memory, online users, shared files, ...</i>		
	Non-Volatile Data: <i>hard disk, tape, dvd, memory card, ...</i>		

Fig. 4. – Data Types

### Networking Data

I dati del traffico di rete, acquisibili dai sistemi attivi e, parzialmente, da quelli in stato *off-line*, potranno consentire agli investigatori di tracciare eventuali attività illecite svolte sul sistema sia da parte dei servizi/delle applicazioni che da parte degli utenti. I dati del traffico di rete potranno essere acquisiti anche prelevando le informazioni, se presenti, direttamente dai *log* degli apparati di sicurezza e di *networking* (*firewall, intrusion detection/ prevention systems, antivirus gateway, network syslog, router, switch, wi-fi access point, ...*) che interessano il perimetro della rete dati oggetto dell'incidente.

### Volatile Data

Prima di procedere allo *shutdown* del sistema, i dati volatili e temporanei, ad esempio quelli presenti all'interno della memoria RAM o le informazioni relative ai processi e servizi in esecuzione, potranno essere salvati con apposite procedure di «*digital forensics*»<sup>16</sup> su dei supporti digitali. Dall'analisi di tali dati gli investigatori potranno recuperare informazioni preziose per la ricerca della prova digitale.

<sup>16</sup> *Digital Forensics*: Con il termine «*digital forensics*» si intende definire un «processo» costituito dall'insieme di misure di carattere legislativo, organizzativo e tecnologico, tese ad analizzare dati e/o informazioni trattati in formato digitale.

### Non-Volatile Data

Probabilmente l'operazione più diffusa nell'ambito della «*digital forensics*» è quella relativa all'acquisizione dei dati non-volatili per la ricerca della c.d. «*digital evidence*» ovvero la prova digitale. I dati non-volatili sono di norma presenti sui supporti di memorizzazione di massa. La loro acquisizione deve avvenire secondo procedure in grado di non alterare il contenuto del supporto originale. L'analisi di tali dati consentirà di ricostruire lo stato del sistema, partendo dall'analisi del dispositivo *hardware* fino ad arrivare all'identificazione di eventuali applicazioni e/o procedure non autorizzate o di documenti/*files* utili alla formazione della prova. Al fine di non distruggere/alterare il supporto originale, tutte le operazioni di analisi andranno condotte sulle copie dei supporti originali acquisiti.

#### 11. Strumenti di supporto e di analisi

Nel caso di una indagine informatica è opportuno che gli investigatori dispongano di una serie di strumenti, siano essi sia *hardware* che *software*, per l'acquisizione e l'analisi della prova digitale. Un laboratorio di analisi per le evidenze digitali è normalmente composto da una serie di strumenti tra i quali quelli per:

1. l'acquisizione dei dati dai vari supporti digitali (SCSI, EIDE, SATA, ...);
2. l'analisi dei dati (*software* commerciale o *open-source*);
3. l'analisi «*live*» dei sistemi;
4. l'analisi del traffico di rete;
5. il supporto agli investigatori.

##### 11.1. Il processo di acquisizione

Per acquisire un supporto informatico in modalità «forense»<sup>17</sup> è necessario utilizzare dei sistemi che siano in grado di eseguire una copia *bit-a-bit*

---

<sup>17</sup> Informatica Forense: L'informatica forense è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici (fonte: *wikipedia*).

dell'originale. Tale operazione è eseguibile solo su un sistema disattivato. Nel caso in cui si abbia il sospetto di un malfunzionamento su di un sistema critico, che per motivi legati alla continuità del servizio non può essere disattivato, è possibile comunque intervenire in modalità cosiddetta «*live*» per effettuare sia l'acquisizione del supporto digitale che le informazioni legate alla *network forensics*. In tale modalità i *tool* di duplicazione e di analisi vengono eseguiti direttamente sul sistema «*target*». I dati così raccolti consentiranno un'analisi approfondita del sistema senza operare direttamente su di esso. Se dal risultato dell'analisi dei dati risultasse la presenza di *software* malevoli e/o applicazioni non autorizzate, allora si potrà procedere con lo *shutdown* programmato del sistema e la successiva acquisizione dei dati, dati che, raccolti su un sistema disattivato, potranno essere valutati anche in sede giuridica. Da segnalare che su sistemi attivi che adottano una tecnologia RAID<sup>18</sup>, in grado cioè di creare un disco logico da un insieme di dischi fisici, la modalità di acquisizione «*live*» può risultare in alcune situazioni l'unica impiegabile. Una ulteriore considerazione nell'esecuzione di una copia «forense» dei supporti riguarda la corretta corrispondenza dai dati presenti nel supporto originale e in quello duplicato. Tale corrispondenza viene garantita da una funzione matematica denominata HASH<sup>19</sup> che genera dei codici univoci. Tale funzione, di norma integrata nei dispositivi *hardware* e *software* di duplicazione, svolge un ruolo essenziale nella «*digital forensics*», ovvero permette all'operatore di verificare la rispondenza tra il supporto originale e quello duplicato. Infatti i due supporti, per essere considerati identici, dovranno avere entrambi un codice *hash* risultante equivalente. Gli strumenti da utilizzare per l'acquisizione dei dati devono essere scelti in base alla tipologia dei supporti utilizzati dall'azienda, così come in base alla tipologia dei *file-systems* adottati deve essere scelto il *software* applicativo di analisi e ricerca delle informazioni. Un laboratorio di analisi forense deve quindi essere attrezzato per poter operare su un ampio *range* di apparecchiature elettroniche ed effettuare analisi

---

<sup>18</sup> RAID: Un *Redundant Array of Independent Disks* («insieme ridondante di dischi indipendenti», RAID) è un sistema informatico che usa un insieme di dischi rigidi per condividere o replicare le informazioni. I benefici del RAID sono di aumentare l'integrità dei dati, la tolleranza ai guasti e/o le prestazioni, rispetto all'uso di un singolo disco (fonte: *wikipedia*).

<sup>19</sup> HASH: Nel linguaggio scientifico, l'*hash* è una funzione univoca operante in un solo senso (ossia, che non può essere invertita), atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di «impronta digitale» del testo in chiaro, e viene detta valore di *hash*, *checksum* crittografico o *message digest* (fonte: *wikipedia*).