Investigazione ed analisi forense

Autore: Andrea Reghelin

Agenda

- ✓ Normative applicabili in Italia
- ✓ La nozione di prova in sede civile penale e lavoristica
- ✓ Valenza della digital forensics a livello processuale
- ✓ Le novità introdotte con la ratifica della convenzione sul cybercrime
- ✓ Profili giuridici della acquisizione, conservazione ed analisi della prova informatica
- ✓ Profili giuridici dei file di log
- ✓ Focus: la digital forensics in ambito aziendale
- ✓ La giurisprudenza rilevante
- ✓ I problemi aperti
- ✓ Contacts, Q&A

Normative applicabili in Italia

Normative applicabili in Italia

- L'essenza della digital forensics consiste nel **definire corrette metodologie atte a preservare, identificare e studiare le informazioni contenute nei sistemi informativi per evidenziare l'esistenza di prove utilizzabili in sede processuale.**

- Molteplici sono i soggetti che potrebbero essere interessati all'utilizzo processuale di una prova informatica. Si pensi per esempio:
  - al **pubblico ministero** che debba provare la colpevolezza di un imputato di un reato in cui l'utilizzo della strumentazione informatica è mezzo o fine dell'attività criminale;
  - all'**imputato** che voglia fornire prove a proprio favore;
  - al **privato (persona fisica o giuridica)** che intenda far valere in giudizio la lesione di un proprio diritto da parte di un terzo, con la conseguente richiesta di un risarcimento del danno in sede civilistica.

Normative applicabili in Italia

- L'esame delle fonti normative applicabili alla digital forensics non può dunque prescindere dalle norme vigenti nel nostro ordinamento in materia di prove.

- La distinzione fondamentale, per enucleare le fonti normative applicabili concernenti le prove, è tra il processo civile e il processo penale.

- Va comunque tenuto presente che in ambito civilistico è necessario altresì considerare le peculiarità in materia di prova previste per il processo del lavoro.

Normative applicabili in Italia

- A titolo esemplificativo, si considerino:
  - il decreto legislativo 30 maggio 2008 n. 109 (Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE);
  - la legge 18 marzo 2008, n. 48 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno)
  - la legge 6 febbraio 2006, n. 38 (Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet);
  - il decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione digitale);
  - il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali);
  - il decreto legislativo 8 giugno 2001, n. 231 (Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300);
  - la legge 3 agosto 1998, n. 269 (Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù);
  - la legge 23 dicembre 1993, n. 547 (Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica);
  - la legge 20 maggio 1970, n. 300 (Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento).

La nozione di prova

La nozione di prova

- Durante il processo, sia in sede civile sia in sede penale, il giudice deve **ricostruire**, sulla base delle prove raccolte, **la verità dei fatti** ai fini della propria decisione.
- La funzione principale della prova è dunque quella di permettere al giudice la corretta ricostruzione e dimostrazione dei fatti affermati dalle parti nel corso del processo.
- La prova informatica (cioè un insieme di informazioni tradotte nel linguaggio utilizzato dalle strumentazioni informatiche non immediatamente intelligibili dall'uomo) assolve alla medesima funzione di tutte le altre prove anche se, per le sue caratteristiche intrinseche, presenta problematiche particolarmente delicate e complesse.
- **In particolare, la facilità con cui tali informazioni possono essere manipolate, alterate o distrutte rende necessarie specifiche procedure per la loro acquisizione e conservazione**.

La nozione di prova in sede civilistica

- L'articolo 115 del Codice di Procedura Civile prevede che, salvi i casi previsti dalla legge il giudice deve porre a fondamento della decisione le prove proposte dalle parti.
- Principio fondamentale del processo civile, quindi, **è che chiunque voglia far valere in giudizio un diritto deve provare i fatti che ne costituiscono il fondamento (principio dell'onere della prova).**
- Parimenti, **incombe sul soggetto che intenda eccepire l'inefficacia di tali fatti, o sostenere che il diritto invocato si è modificato o estinto, provare a sua volta i fatti su cui si fonda la sua eccezione**.
- La prova è dunque sostanzialmente la dimostrazione della veridicità dei fatti che ciascuna parte chiede al giudice di accertare ai fini dell'ottenimento di un provvedimento a essa favorevole.
- **La mancata dimostrazione di un fatto sul quale la parte ha l'onere della prova comporta necessariamente la soccombenza su quel punto.**

La nozione di prova in sede civilistica

- All'interno del processo civile assumono grande rilevanza **le prove precostituite**, così definite perché hanno la caratteristica di essere state formate al di fuori del processo e di entrarvi per effetto della loro produzione a opera delle parti (tipiche sono le prove documentali).
- Le principali prove precostituite sono le seguenti:
  - **Atto pubblico**. In base all'articolo 2699 c.c., è il documento redatto, con le richieste formalità, da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è formato.
  - **Scrittura privata**. È il documento munito di sottoscrizione autografa che, ai sensi dell'articolo 2702 c.c., fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta.
  - **Riproduzioni meccaniche**. Sono definite dall'articolo 2712 c.c. come le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose. Formano piena prova dei fatti e delle cose rappresentate se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime

La nozione di prova in sede civilistica

- Il documento informatico
  - In materia di prove precostituite è necessario fare un breve cenno alla disciplina del documento informatico attualmente contenuta nel Codice dell'Amministrazione digitale (decreto legislativo 7 marzo 2005, n. 82).
  - L'articolo 1 di detto codice definisce innanzitutto il documento informatico come "**la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti**".
  - **Quindi il documento informatico, cui è stato chiaramente riconosciuto dalla legge un valore probatorio, può essere validamente prodotto in giudizio come prova ed essere valutato dal giudice**.
  - L'articolo 20 comma 1 bis del Codice stabilisce inoltre che l'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
  - Quando però il **documento informatico** è sottoscritto **con firma digitale o con un altro tipo di firma elettronica qualificata**, lo stesso **assume l'efficacia prevista dall'articolo 2702 c.c**., ovvero l'efficacia di una scrittura privata (art. 22 comma 1 d.lgs 82/2005).

La nozione di prova in sede penalistica

- L'articolo 111 della Costituzione, contiene le disposizioni fondamentali del processo penale ed è quindi il punto di partenza per poterne comprendere le caratteristiche.

- Ciò che rileva ai nostri fini, in particolare, **è il principio del contraddittorio nella formazione della prova**, in base al quale la stessa deve formarsi dialetticamente con l'altra parte nei cui confronti può essere fatta valere.

La nozione di prova in sede penalistica

- Il giudice, quando è richiesto, può assumere prove non disciplinate dalla legge nel caso risultino idonee ad assicurare l'accertamento dei fatti e non pregiudichino la libertà morale della persona (art. 189 c.p.p.).

- Il codice di procedura penale, quindi, **non prevede un principio di tassatività dei mezzi di prova, consentendo invece al giudice di ammettere prove che non siano direttamente disciplinate dalla legge, purché le stesse siano idonee a risalire alla verità dei fatti e non siano lesive della libertà morale della persona**.

- La Corte di Cassazione Penale, in punto, ha precisato che il giudice, nell'assumere prove non disciplinate dalla legge a norma dell'articolo 189 c.p.p., è tenuto ad applicare i criteri legali stabiliti per gli analoghi mezzi di prova tipici, ovvero a ricorrere a consolidate massime di esperienza o regole di inferenza secondo una disciplina scientifica (Cass. Pen. 12 dicembre 1999, n. 1858).

La nozione di prova in sede penalistica

- In relazione ai criteri di ammissione delle prove, l'articolo 190 c.p.p. prevede che le stesse **sono ammesse a richiesta delle parti alle quali è riconosciuto esplicitamente un diritto alla prova**. La legge, tuttavia, stabilisce i casi nei quali le prove possono essere ammesse d'ufficio dal giudice.

- Fondamentale in tal senso è la disposizione di cui all'articolo 191 c.p.p., in base al quale "**le prove acquisite in violazione dei divieti stabiliti dalla legge non possono essere utilizzate**".
  - Il rispetto delle norme in materia di ammissione o di acquisizione probatoria assume una fondamentale importanza per scongiurare che una prova venga dichiarata inutilizzabile.
  - Lo stesso articolo prevede, d'altra parte, che "**l'inutilizzabilità è rilevabile anche di ufficio in ogni stato e grado del procedimento**", impedendo quindi che il vizio possa essere in qualche modo successivamente sanato.

La nozione di prova in sede penalistica

- La valutazione delle prove
  - Principio fondamentale è quello del libero convincimento del giudice.

  - L'articolo 192 c.p.p., stabilisce, tuttavia, che **il giudice debba valutare la prova dando conto nella motivazione dei risultati acquisiti e dei criteri adottati.**

    Il giudice deve dunque esporre nelle motivazioni le ragioni del proprio convincimento ovvero l'iter logico seguito per trarre determinate conclusioni dalle prove a sua disposizione.

    Questa norma ha la funzione di non rendere assolutamente discrezionale la valutazione del giudice, permettendo invece una verifica del ragionamento dallo stesso effettuato nella valutazione delle prove.

La nozione di prova in sede penalistica

- I mezzi di prove e di ricerca della prova
  - I **mezzi di prova** sono gli elementi direttamente utilizzabili dal giudice ai fini della formazione del suo libero convincimento.

    Testimonianza, esperimenti giudiziali perizia, prove documentali, ..
  - I **mezzi di ricerca della prova**, invece, sono strumenti di indagine che consentono di acquisire la prova.

    Ispezioni, perquisizioni, sequestri, intercettazione di comunicazioni, ..

- Ne consegue che le norme sui mezzi di prova si rivolgono prevalentemente al giudice mentre quelle sui mezzi di ricerca della prova si rivolgono al Pubblico Ministero (e per quanto di competenza alla polizia giudiziaria).

La nozione di prova in sede penalistica

- **Le indagini difensive**
  - Il nuovo Codice di Procedura Penale entrato in vigore nel 1988 ha valorizzato il principio di parità tra accusa e difesa, attribuendo ai difensori la facoltà di svolgere attività investigative al fine di ricercare elementi di prova in favore dei propri assistiti.
  - Tuttavia, solo con l'approvazione della legge 7 dicembre 2000, n. 397 (Disposizioni in materia di indagini difensive) **l'attività investigativa del difensore è stata dettagliatamente procedimentalizzata** e ha quindi ottenuto un riconoscimento che è oggi possibile definire completo.
  - Le norme che riguardano le investigazioni difensive introdotte dalla legge 397/2000 sono contenute nel titolo VII del libro quinto del Codice di Procedura Penale agli articoli da 391 bis a 391 decies.

La nozione di prova nel processo del lavoro

- Si è evidenziato in precedenza come nel processo civile viga il principio della corrispondenza tra il chiesto e il pronunciato (art. 112 c.p.c.) e come l'articolo 115 c.p.c. preveda che il giudice (salvo i casi disciplinati dalla legge) debba porre a fondamento della sua decisione le prove proposte dalle parti (principio dell'onere della prova).
- I medesimi principi non possono dirsi operanti in modo assoluto nel rito del lavoro posto che l'articolo 421 c.p.c. attribuisce allo stesso alcune facoltà ulteriori, ovvero:
  - indicare alle parti in ogni momento le irregolarità degli atti e dei documenti che possono essere sanate assegnando un termine per provvedervi, salvo gli eventuali diritti quesiti;
  - disporre d'ufficio in qualsiasi momento l'ammissione di ogni mezzo di prova, anche fuori dei limiti stabiliti dal Codice Civile, a eccezione del giuramento decisorio;
  - richiedere informazioni e osservazioni, sia scritte sia orali, alle associazioni sindacali indicate dalle parti
  - disporre, su istanza di parte, l'accesso sul luogo di lavoro, perché necessario al fine dell'accertamento dei fatti, e disporre altresì, se ne ravvisa l'utilità, l'esame dei testimoni sul luogo stesso;
  - ordinare, qualora lo ritenga necessario, la comparizione, per interrogarle liberamente sui fatti della causa, anche di quelle persone che siano incapaci di testimoniare

Valenza della digital forensics a livello processuale

Valenza della digital forensics a livello processuale

- Essenziale perché una prova sia ammessa nel processo, civile o penale, e venga successivamente valutata dal giudice in favore della parte che l'ha prodotta o richiesta, **è la sua idoneità a dimostrare i fatti ai quali si riferisce**.
- In un contesto informatico caratterizzato dall'elevato rischio di alterazione delle informazioni o dei dati conservati o scambiati dai sistemi informatici e telematici, le precauzioni che le parti sono tenute ad adottare ai fini di conservare il valore probatorio degli elementi raccolti sono di gran lunga superiori rispetto ad altri contesti.
- La prova informatica dunque, ai fini della sua utile utilizzazione in sede processuale, dovrà necessariamente possedere alcuni requisiti, in particolare **l'integrità e non ripudiabilità dell'elemento raccolto**.
- In particolare, l'integrità può essere definita come "quella proprietà per effetto della quale si escludono alterazioni indebite delle tracce informatiche intervenute in epoca successiva alla creazione, trasmissione o allocazione in un supporto autorizzato" (G. Costabile).

Valenza della digital forensics a livello processuale

- In ogni caso, indipendentemente da chi stia agendo, l'acquisizione degli elementi di prova deve avvenire in modo tale da non compromettere l'integrità e la genuinità degli elementi raccolti per non impedire il loro futuro ed eventuale utilizzo in sede processuale
- Al fine di acquisire elementi probatori che risultino, nei limiti del possibile, utilizzabili dal magistrato in ogni sede, dovendo garantire l'integrità e la non ripudiabilità, è bene quindi che nell'acquisizione degli elementi di prova vengano utilizzate **metodologie di digital forensics** che si fondino sulle più avanzate procedure riconosciute a livello internazionale e che le stesse siano formalizzate, così come ogni passaggio di un'attività di Digital Forensics, e pedissequamente rispettate
- Profilo fondamentale in ogni fase delle attività di digital forensics è **costituito inoltre dalla corretta documentazione** (la cosiddetta chain of custody o catena di custodia) **operazioni effettuate (cronologia di tutte le operazioni compiute, identificazione e descrizione dei supporti e azioni intraprese per la custodia di ciascuno di essi)**.

Valenza della digital forensics nel processo civile

- Come visto è onere delle parti produrre al giudice le prove che confermano l'esistenza del diritto che si vuole riconosciuto dal giudice: **la mancata prova di un diritto comporta la soccombenza**.
- Nel caso di prove informatiche, quindi, è onere della parte raccoglierle e conservarle in modo tale che non vi sia il rischio che le stesse vengano considerate inidonee a dimostrare il fatto invocato.
- **Molto spesso le prove informatiche, prima della loro individuazione, sono conservate su supporti di proprietà del soggetto che agisce in giudizio per far valere un proprio diritto.**
- La prova informatica entrerà nel processo civile essenzialmente **come una prova documentale**, ma il suo valore probatorio è conseguenza delle modalità con le quali è stata acquisita e nella sua idoneità a provare i fatti ai quali si riferisce.
- **Le prove informatiche prodotte in giudizio, seppur raccolte con le metodologie proprie della digital forensics, sono comunque il frutto di un'attività di parte e non hanno un pieno valore probatorio, ma sono liberamente valutabili dal giudice**.

Valenza della digital forensics nel processo penale

- Si pongono i problemi della sorte processuale delle evidenze informatiche raccolte senza adottare idonee metodologie riconosciute a livello internazionale, soprattutto in seguito alle modifiche apportate dalla legge n. 48/2008 al Codice di Procedura Penale in relazione agli articoli riguardanti i mezzi di ricerca della prova e in particolare le ispezioni, le perquisizioni e i sequestri.
- La soluzione che appariva più coerente con i principi che regolano le prove nel processo penale, anche anteriormente alle suddette modifiche, era quella della loro **inutilizzabilità in sede processuale** in virtù del fatto che le stesse non sono idonee a garantire l'integrità e genuinità degli elementi raccolti e pertanto ad accertare i fatti di reato.
- Si anticipa, comunque che le nuove norme prevedono nelle attività di ispezione perquisizione e sequestro "*l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*". L'adozione di tali misure tecniche è ora prevista direttamente dalle norme contenute nel c.p.p. e la loro mancata attuazione (ovvero senza utilizzare le metodologie proprie della Digital Forensics) comporterà l'inutilizzabilità delle evidenze informatiche raccolte non correttamente.

Valenza della digital forensics nel processo penale

- Nel campo della digital forensics, un ulteriore problema da affrontare è quello **dell'assenza di uno standard universalmente riconosciuto nonché di tecniche di indagine che si possano considerare consolidate**.
- Tale assenza comporta sempre un esito incerto circa l'utilizzabilità e la valenza probatoria dei risultati delle attività di indagine compiute, indipendentemente da come siano state nel concreto effettuate.
- Nel processo penale il giudice ha però il compito di verificare nel caso concreto il valore probatorio delle prove informatiche presentate dalle parti che discende, come visto, dalla possibilità di accertare l'utilizzo di metodi di indagine, in ottemperanza a regole tecniche riconosciute che diano la garanzia della integrità e genuinità degli elementi raccolti.
- L'utilizzo delle metodologie proprie della digital forensics, seppure in assenza di una garanzia circa l'esito processuale delle stesse, è attualmente l'unica scelta possibile.
- Anche in relazione a questo aspetto è auspicabile che le modifiche introdotte dalla legge 48/2008 costituiscano il presupposto per la nascita di metodologie condivise per l'effettuazione delle operazioni di acquisizione, conservazione e analisi delle evidenze informatiche, così come avviene per altre tecniche di indagine di carattere scientifico.

Le novità introdotte con la ratifica della convenzione sul cybercrime

Le novità introdotte con la ratifica della convenzione sul cybercrime

- Nel contesto penale l'autorità giudiziaria, durante la fase delle indagini preliminari, dispone di alcuni mezzi di ricerca della prova e in particolare delle ispezioni, delle perquisizioni e dei sequestri.
- **L'ispezione** (art. 244 c.p.p.), è l'attività di polizia giudiziaria attraverso la quale vengono descritte le tracce e gli altri effetti materiali del reato
- La **perquisizione** (art. 247 c.p.p.) ha invece lo scopo di ricercare il corpo del reato e le cose pertinenti al reato. Tale attività è prodromica al successivo sequestro.
- Il **sequestro** è l'attività mediante la quale vengono prelevate dall'autorità giudiziaria il corpo del reato e le cose pertinenti al reato necessarie per l'accertamento dei fatti (art. 253 c.p.p.).
  - Il corpo del reato sono le cose sulle quali o mediante le quali il reato è stato commesso, nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo
  - La nozione di "cose pertinenti al reato" comprende invece le cose che sono in rapporto indiretto con la fattispecie concreta e sono strumentali, secondo i principi generali della libera prova e del libero convincimento del giudice, all'accertamento dei fatti.

Le novità introdotte con la ratifica della convenzione sul cybercrime

- **Parte della dottrina riteneva che l'ispezione e la perquisizione fossero strumenti che sono idonei a comprendere al loro interno l'attività di apprensione dei dati digitali.**
- Come si è accennato in precedenza l'anno scorso è entrata in vigore **la legge n. 48 del 18 marzo 2008** recante "***Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno***". Questa legge riveste una grande importanza per la tematica della digital forensics ed in estrema sintesi prevede:
  - alcune modifiche al Codice Penale concernenti la criminalità informatica (inserimento di nuove fattispecie di reato e aggiornamento di alcuni articoli già presenti);
  - L'inclusione di "delitti informatici e trattamento illecito di dati" nel catalogo dei reati per i quali è prevista la responsabilità amministrativa degli enti ai sensi del decreto legislativo 8 giugno 2001, n. 231;
  - alcune modifiche al Codice di Procedura Penale volte rendere obbligatorio per le forze di polizia l'utilizzo di specifiche metodologie nel corso delle indagini informatiche (per esempio modifiche in materia di ispezione e perquisizione);
  - la modifica di parte della disciplina sulla *data retention contenuta nell'art. 132 del d.lgs* 196/2003.

Principali modifiche in materia di crimini informatici

Alcune novità introdotte dalla legge n. 48 del 18 marzo 2008		
Articolo del codice penale	**Vecchia formulazione**	**Nuova formulazione**
491 bis - Documenti informatici.	Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.	Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.
615 quinquies - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)	Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a 10.329 euro	Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329

Principali modifiche in materia di crimini informatici

Alcune novità introdotte dalla legge n. 48 del 18 marzo 2008		
Articolo del codice penale	**Vecchia formulazione**	**Nuova formulazione**
Art. 635-bis - Danneggiamento di informazioni, dati e programmi informatici.	1. Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. 2. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.	1. Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. 2. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio

Principali modifiche in materia di crimini informatici

Alcune novità introdotte dalla legge n. 48 del 18 marzo 2008		
Articolo del codice penale	**Vecchia formulazione**	**Nuova formulazione**
Art. 635-ter - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità).	-	1. Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. 2. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.
Art. 635-quater -Danneggiamento di sistemi informatici o telematici	-	1. Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. 2. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Le novità introdotte con la ratifica della convenzione sul cybercrime

- Il legislatore italiano, seppur con le integrazioni che prenderemo in esame, ha dunque deciso di mantenere gli istituti dell'ispezione e della perquisizione per le attività di apprensione dei dati digitali

- In materia di ispezione la legge n. 48/2008 ha previsto un allargamento delle attività ispettive previste dall'articolo 244 c.p.p. stabilendo che l'autorità giudiziaria possa disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica "***anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione***".

Le novità introdotte con la ratifica della convenzione sul cybercrime

- In materia di perquisizione viene aggiunto un nuovo comma (1 bis) all'articolo 247 c.p.p. in base al quale "*Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza,* ***ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione***".

Le novità introdotte con la ratifica della convenzione sul cybercrime

- In relazione alle attività ad iniziativa della polizia giudiziaria la l. 48/2008 modifica gli articoli 352, 353 2 354 del codice di procedura penale.
- All'articolo 352 c.p.p. il nuovo comma 1 bis prevede che "***Nella flagranza del reato, ovvero nei casi di cui al comma 2*** (es. esecuzione di un'ordinanza che dispone la custodia cautelare, fermo di una persona indiziata di delitto.) ***quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi".***

Le novità introdotte con la ratifica della convenzione sul cybercrime

- In relazione all'acquisizione di plichi o di corrispondenza l'articolo 353 c.p.p. prevede ora che:
  - se ha fondato motivo di ritenere che i plichi contengano notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo, l'ufficiale di polizia giudiziaria informa col mezzo più rapido il pubblico ministero il quale può autorizzarne l'apertura immediata ***" e l'accertamento del contenuto"***
  - Se si tratta di "***lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica***" per i quali è consentito il sequestro a norma dell'articolo 254, gli ufficiali di polizia giudiziaria, in caso di urgenza, ordinano a chi è preposto al servizio postale, "***telegrafico, telematico o di telecomunicazione***" di sospendere l'inoltro. Se entro quarantotto ore dall'ordine della polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati

Le novità introdotte con la ratifica della convenzione sul cybercrime

- La legge n. 48/2008 approvato integra altresì l'art. 354 c.p.p. (Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro) in base al quale:
  1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.
  2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti. "***In relazione ai dati,alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità".***

Le novità introdotte con la ratifica della convenzione sul cybercrime

- In relazione al sequestro l'art 254 c.p.p. (sequestro di corrispondenza) come modificato dalla l. 48/2008 prevede che:
  - presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, "***anche se inoltrati per via telematica***", che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato;
  - Quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli o "***alterarli***" e senza prendere altrimenti conoscenza del loro contenuto.

Le novità introdotte con la ratifica della convenzione sul cybercrime

- Con riferimento alla custodia delle cose sequestrate le modifiche introdotte (art 260 c.p.p.) prevedono che:
  - Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste ovvero, in relazione alla natura delle cose, con altro mezzo, "***anche di carattere elettronico o informatico"*** idoneo a indicare il vincolo imposto a fini di giustizia
  - L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti. "***Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria***"

Le novità introdotte con la ratifica della convenzione sul cybercrime

- Con riferimenti alla custodia delle cose sequestrate le modifiche introdotte prevedono inoltre che:
  - "*Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria*" (art. 259 c.p.p.).

Profili giuridici della acquisizione, conservazione ed analisi della prova informatica: problematiche legate al contesto penale

Il sequestro: alcune considerazioni (1)

- In relazione al sequestro ad oggetto informatico, occorre tuttavia prendere in considerazione il fatto che le strumentazioni informatiche e telematiche solitamente non sono solo uno strumento utilizzato per commettere un reato (o l'oggetto del reato), ma hanno spesso un'importanza fondamentale per il soggetto che ne ha la disponibilità (si pensi al contesto aziendale).
- Una lettura attenta dell'articolo 253 c.p.p. non consente un sequestro delle cose che non costituiscono il corpo del reato o che non sono pertinenti al reato.
- Troppo spesso accade invece che, per imperizia o superficialità nella valutazione, vengano poste sotto sequestro anche strumentazioni che non contengono elementi utili all'indagine, con grave pregiudizio del soggetto destinatario dell'attività di sequestro.
- Non tutte le strumentazioni informatiche hanno la funzionalità di poter conservare informazioni e il loro sequestro si rivela inutile ai fini dell'attività d'indagine ma dannoso dal punto di vista economico per il destinatario, che potrebbe anche essere un soggetto terzo estraneo alla commissione del reato.

Il sequestro: alcune considerazioni (2)

- Come rilevato dalla dottrina (Andrea Monti "No ai sequestri indiscriminati di computer", in *Diritto dell'Internet, 2007, 3),* mentre il sequestro dell'elaboratore si rivela nella maggioranza dei casi inutile, quello delle periferiche potrebbe trovare la propria giustificazione per l'effettuazione di rilievi dattiloscopici o per ricercare campioni biologici per tentare di individuare l'identità dell'utilizzatore del computer. Il sequestro delle periferiche, dunque, lungi dall'essere sempre indispensabile per le indagini, potrebbe diventarlo solo nei casi in cui fosse necessario compiere, per esempio, le suddette analisi.

Profili giuridici della acquisizione, conservazione ed analisi della prova informatica: problematiche legate al contesto penale

- La via preferibile, in materia di ricerca degli elementi di prova contenuti su supporti informatici, è quindi la loro acquisizione in modalità ripetibile. **In sintesi, sia le attività di acquisizione dei dati digitali sia le successive fasi di elaborazione e analisi degli stessi non devono alterare i dati originali**.

- Questo comporta il compimento delle attività di analisi delle tracce informatiche non sul supporto originale sequestrato, ma su immagini dello stesso create mediante appositi strumenti hardware e software che garantiscono l'esatta corrispondenza con l'originale.

- Vantaggio di questo sistema è la preservazione del supporto originale, che deve essere conservato adottando tutte le idonee contromisure per evitarne l'alterazione (apposizione di sigilli, conservazione in luogo sicuro ecc.), e il compimento di tutte le attività di analisi su una "bit stream image" dello stesso, senza compromissione dei diritti della difesa, che potrà in ogni momento effettuare proprie controanalisi.

Profili giuridici della acquisizione, conservazione ed analisi della prova informatica: problematiche legate al contesto penale

- In campo penalistico la problematica della ripetibilità delle operazioni di digital forensics nelle fasi successive del procedimento è di estrema rilevanza.
- E' quindi opportuno fare qualche considerazione sull'attività di indagine del Pubblico Ministero e **in particolare agli accertamenti tecnici**, che assumono grande rilevanza nel contesto della digital forensics.
  - L'articolo 359 c.p.p. prevede che il Pubblico Ministero, quando procede ad accertamenti per cui sono necessarie specifiche competenze, possa nominare e avvalersi di consulenti che non possono rifiutare la loro opera.
  - **Per accertamento, non deve intendersi la constatazione o la raccolta di dati materiali pertinenti al reato e alla sua prova, ma il loro studio e la relativa elaborazione critica.**

Profili giuridici della acquisizione, conservazione ed analisi della prova informatica: problematiche legate al contesto penale

- Tipico caso di accertamento è **l'attività di apprensione del dato digitale** e la sua **successiva analisi**.

- In merito a tale tipologia di accertamenti si discute in dottrina se gli stessi, anche nel caso di utilizzo delle metodologie proprie della digital forensics, abbiano o meno natura irripetibile ai fini dell'applicazione dell'articolo 360 c.p.p.(accertamenti tecnici non ripetibili). Occorre valutare in altri termini se tali attività di apprensione ed analisi non comportino una modificazione dei dati digitali originari.

- In base a tale norma quando gli accertamenti riguardano persone, cose o luoghi il cui stato è soggetto a modificazione, **il Pubblico Ministero deve avvisare senza ritardo la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico ai propri consulenti e della facoltà di nominare a loro volta consulenti tecnici**.

- **L'effettuazione di un accertamento tecnico irripetibile senza il rispetto degli adempimenti di cui sopra comporta la sanzione dell'inutilizzabilità dei risultati dello stesso in sede dibattimentale.**

Profili giuridici della acquisizione, conservazione ed analisi della prova informatica: problematiche legate al contesto penale

- E' quindi necessario che le stesse attività di creazione dell'immagine del supporto (in caso di accertamento ripetibile ex art. 359 c.p.p.) siano poste in essere con strumenti tali che consentano di escludere qualsiasi modificazione del supporto originale e la corrispondenza tra lo stesso e la copia generata.
- Qualsiasi modificazione renderebbe infatti tale attività un accertamento irripetibile posto in essere in assenza delle garanzie previste dal codice di procedura penale e renderebbe inutilizzabile la prova raccolta all'interno del processo.
- Secondo parte della dottrina l'utilizzo da parte degli organi inquirenti di software "proprietari" potrebbe costituire un problema in quanto non essendo possibile verificare il loro concreto funzionamento non vi sarebbero garanzie di fedeltà all'originale della copia generata (possibili eccezioni difensive).

I profili giuridici dei file di log

I profili giuridici dei file di log

- file di log sono dei comuni file di testo prodotti, conservati e generati automaticamente dal sistema, all'interno dei quali è possibile rilevare le tracce di ogni attività compiuta (in entrata ed in uscita).
  - Comunicazioni (file di log del *provider* che concede l'accesso alla rete).
  - File di log del provider che ospita il sito web sul quale un utente sta navigando.
  - File di log del servizio che viene utilizzato (ad esempio una sessione di chat).
  - File di log dell'accesso alla casella di posta elettronica etc.

I profili giuridici dei file di log

- I file di log rivestono un'importanza fondamentale sia nel processo civile sia nel processo penale.
- Sotto un profilo penalistico, trattasi di elementi che possono risultare utili sia ai fini delle indagini del Pubblico Ministero sia in relazione alla posizione delle altre parti coinvolte nel processo.
- Dall'esame dei file di log si possono ricavare fondamentali informazioni (in particolare per risalire al soggetto che ha usufruito di un dato servizio o che ha compiuto determinate operazioni con l'utilizzo delle strumentazioni informatiche e telematiche a sua disposizione).
- È bene considerare che nel nostro ordinamento giuridico non esiste un obbligo generalizzato di conservazione dei file di log prodotti dai sistemi informatici e telematici.

I profili giuridici dei file di log

- Gli unici obblighi di conservazione dei dati del traffico telematico sono stati originariamente previsti in capo ai fornitori di servizi comunicazione elettronica dal decreto legge 27 luglio 2005, n. 144 convertito in legge 31 luglio 2005, n. 155 attraverso il quale sono state adottate nel nostro ordinamento alcune misure urgenti per il contrasto del terrorismo internazionale che hanno un'incidenza diretta sulla fornitura di servizi di comunicazione
- Si ricorda che, in base al decreto legislativo 30 giugno 2003, n. 196, prima dell'adozione delle misure urgenti antiterrorismo dovevano essere conservati obbligatoriamente dai fornitori per finalità di accertamento e repressione dei reati solo i dati del traffico telefonico. Ai fornitori di servizi di comunicazione elettronica era comunque lasciata la possibilità di conservare per un periodo non superiore a sei mesi i dati strettamente necessari alla fatturazione dei servizi erogati ai clienti, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento e salva l'ulteriore specifica conservazione necessaria per effetto di contestazione anche in sede giudiziale (art. 123 d.lgs 196/03).

I profili giuridici dei file di log

- L'articolo 132 del d.lgs. 196/2003 come modificato dalla legge 31 luglio 2005, n. 155 aveva previsto nuove regole in materia di conservazione dei dati per il traffico telefonico e telematico, e in particolare:
  - i dati relativi al traffico telefonico inclusi quelli concernenti le chiamate senza risposta dovevano essere conservati dal fornitore per ventiquattro mesi, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, dovevano essere conservati dal fornitore per sei mesi (art. 132 comma 1);
  - decorso il termine di cui al punto precedente, i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, dovevano essere conservati dal fornitore per ulteriori ventiquattro mesi e quelli relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, devono conservati per ulteriori sei mesi in riferimento a particolari tipologie di reato.

I profili giuridici dei file di log

- La previsione di un obbligo di conservazione dei dati relativi al traffico telematico, seppur accolta positivamente, non ha comunque mancato di suscitare qualche perplessità in relazione ad alcuni aspetti.
- In particolare, è stato rilevato come **il termine di 6 mesi previsto per la conservazione in relazione ai reati generici sia troppo breve** in quanto non prende in considerazione la possibilità di accertamenti complessi relativi a reati commessi attraverso la rete.
- Inoltre **non erano state disciplinate le modalità di conservazione dei dati di traffico telematico da parte dei fornitori di servizi di comunicazione e di acquisizione dei file di log da parte della polizia giudiziaria.**
  - Il problema, infatti, è la garanzia circa l'integrità dei dati conservati dai fornitori di servizi di comunicazione elettronica nonché le modalità di estrapolazione dei dati che si riferiscono all'indagine.

I profili giuridici dei file di log

- Sul tema relativo agli obblighi di conservazione dei dati di traffico telefonico e telematico sono avvenute importanti modifiche nel corso del 2008, **dapprima con la legge n. 48/2008 e poi con il D.Lgs 109/2008**.
- La **norma di riferimento rimane l'art. 132 del D.Lgs 196/2003**, come modificato dalle norme sopra elencate, il quale prescrive, come visto, alcuni obblighi di conservazione dei dati di traffico telefonico e telematico in capo ai fornitori di servizi di comunicazione elettronica.

I profili giuridici dei file di log

- E’ importante fare chiarezza sui soggetti tenuti ad adempiere a tali prescrizioni.
- Il Garante per la protezione dei dati personali, nel provvedimento generale del 17 gennaio 2008 (così come modificato in data 24 luglio 2008), avente ad oggetto la “sicurezza dei dati di traffico telefonico e telematico”, **ha definito il termine "fornitore" utilizzato dall’art. 132 del D.Lgs 196/2003 per indicare il destinatario degli obblighi di conservazione dei dati di traffico, individuandolo nel soggetto che mette a disposizione del pubblico servizi di comunicazione elettronica su reti pubbliche di comunicazione.**
- Sono, quindi, tenuti alla conservazione dei dati ai sensi del medesimo art. 132 solo i soggetti che “***realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione***”.

I profili giuridici dei file di log

- Il medesimo provvedimento del Garante **specifica ulteriormente che non sono soggetti agli obblighi di data retention**:
  - i soggetti che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche);
  - i soggetti che, pur offrendo servizi di comunicazione elettronica accessibili al pubblico, non generano o trattano direttamente i relativi dati di traffico;
  - i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso a Internet utilizzando tecnologia senza fili, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale;
  - i gestori dei siti Internet che diffondono contenuti sulla rete (c.d. *"content provider"*);
  - i gestori di motori di ricerca.

I profili giuridici dei file di log

- Gli attuali obblighi di data retention disciplinati dall'art. 132 del d.lgs 196/2003 sono i seguenti:
  - i dati relativi al traffico telefonico (diversi da quelli trattati a fini di fatturazione) devono essere conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati; **per le medesime finalità, i dati relativi al traffico telematico, esclusi i contenuti delle comunicazioni, devono essere conservati dal fornitore per dodici mesi dalla data della comunicazione** (art. 132 comma 1 D.Lgs 196/2003);
  - i dati relativi alle chiamate senza risposta (prima assoggettati alla medesima disciplina di cui al punto a.), che siano trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, devono essere conservati per trenta giorni (art. 132 comma 1-bis D.Lgs 196/2003).

I profili giuridici dei file di log

- Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private.
- Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall' articolo 391-quater del codice di procedura penale , ferme restando le condizioni di cui all' articolo 8 , comma 2, lettera f). per il traffico entrante

I profili giuridici dei file di log

- Atra importante novità introdotta dal d.lgs. 109/2008 riguarda specificamente la tipologia dei dati soggetti agli obblighi di data retention.
- Mentre in precedenza la normativa di riferimento indicava genericamente tutti i dati relativi al traffico telefonico e telematico, esclusi i contenuti delle comunicazioni, ora l'articolo 3 del d.lgs. citato contiene la specifica indicazione di quali dati devono essere conservati dagli operatori di telefonia e di comunicazione.
- Accanto a queste norme, il Garante, con il provvedimento del 17 gennaio 2008 (come modificato in data 24 luglio 2008), prescrive, inoltre, ai fornitori di servizi di comunicazione elettronica accessibili al pubblico specifiche misure e accorgimenti da adottare (entro il 31 marzo 2009) a garanzia dei soggetti cui appartengono i dati di traffico oggetto del trattamento, nell'ambito della conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e repressione di reati.

I profili giuridici dei file di log

- Le ragioni che hanno invece indotto il Garante per la protezione dei dati personali ad intervenire sulla questione concernente le modalità di conservazione dei dati di traffico telefonico e telematico sono in particolare le seguenti:
  - il trattamento dei dati di traffico telefonico e telematico presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.
  - i dati relativi al traffico telefonico e telematico dovrebbero riguardare solo alcune caratteristiche esteriori di conversazioni, chiamate e comunicazioni, senza permettere di desumerne i contenuti.
  - l'intensità dei flussi di comunicazione comporta la formazione e, a volte, la conservazione di innumerevoli informazioni che consentono di ricostruire nel tempo intere sfere di relazioni personali, professionali, commerciali e istituzionali, e di formare anche delicati profili interpersonali.

I profili giuridici dei file di log

- Il Garante ha inoltre rilevato che **per le comunicazioni telematiche si pongono ulteriori e più specifiche criticità rispetto alle comunicazioni telefoniche tradizionalmente intese**, in quanto il dato apparentemente "esterno" a una comunicazione (ad es., una pagina *web* visitata o un indirizzo Ip di destinazione) spesso identifica o rivela nella sostanza anche il suo contenuto: può permettere, quindi, non solo di ricostruire relazioni personali e sociali, ma anche di desumere particolari orientamenti, convincimenti e abitudini degli interessati.
- Emerge quindi, secondo il Garante la **necessità**, in attuazione di quanto previsto per legge, **di assicurare che la conservazione di tali dati da parte dei fornitori, laddove essa sia necessaria per prestare un servizio o in quanto imposta dalla legge, avvenga comunque in termini adeguati per garantire una tutela maggiormente efficace dei diritti e delle libertà delle persone.**

I profili giuridici dei file di log

- Il Garante è stato preposto per disposizione di legge a individuare **accorgimenti e misure da porre a garanzia degli interessati** nell'ambito della conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e repressione di reati (art. 132, comma 5 del Codice – D.lgs 196/2003).
- A tal fine, il Garante ha curato preliminarmente diversi approfondimenti tecnici con esperti del settore, nonché numerosi accertamenti ispettivi presso primari fornitori di servizi di comunicazione elettronica ed ha, infine, indetto una specifica consultazione pubblica su un articolato documento indicante le misure e gli accorgimenti ritenuti idonei per la conservazione dei dati di traffico per finalità di giustizia.
- **Nel Provvedimento in esame il Garante ha infine indicato gli accorgimenti e le misure prescritte ai fornitori di servizi di comunicazione elettronica accessibili al pubblico.**

I profili giuridici dei file di log

Principali misure ed accorgimenti per la conservazione dei dati di traffico per finalità di accertamento e prevenzione dei reati, prescritti dal Garante nel provvedimento del 17 gennaio 2008	
Sistemi di autenticazione	Il trattamento dei dati di traffico telefonico e telematico da parte dei fornitori deve essere consentito **solo agli incaricati** del trattamento e unicamente sulla base del preventivo utilizzo di **specifici sistemi di autenticazione informatica basati su tecniche di strong authentication**, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti.
	Per i dati di traffico conservati per esclusive finalità di accertamento e repressione dei reati (cioè quelli generati da più di sei mesi, oppure la totalità dei dati trattati per queste finalità se conservati separatamente dai dati trattati per le altre finalità fin dalla loro generazione), **una di tali tecnologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato**, in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento.
	Tali modalità di autenticazione devono essere applicate anche a tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore.

I profili giuridici dei file di log

Principali misure ed accorgimenti per la conservazione dei dati di traffico per finalità di accertamento e prevenzione dei reati, prescritti dal Garante nel provvedimento del 17 gennaio 2008	
Sistemi di autorizzazione	Relativamente ai sistemi di autorizzazione devono essere adottate **specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati**. Tali differenti funzioni non possono essere attribuite contestualmente a uno stesso soggetto.
	I profili di autorizzazione da definire e da attribuire agli incaricati devono differenziare le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati **distinguendo**, tra queste ultime, **gli incaricati abilitati al solo trattamento dei dati di cui al primo periodo di conservazione obbligatoria** (art. 132, comma 1, del Codice), **dagli incaricati abilitati anche al trattamento dei dati di cui al secondo periodo di conservazione obbligatoria** (art. 132, comma 2, del Codice) e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice).

I profili giuridici dei file di log

Principali misure ed accorgimenti per la conservazione dei dati di traffico per finalità di accertamento e prevenzione dei reati, prescritti dal Garante nel provvedimento del 17 gennaio 2008	
Conservazione separata	I **dati di traffico conservati per esclusive finalità di accertamento e repressione di reati vanno trattati necessariamente tramite sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità**, sia nelle componenti di elaborazione, sia nell'immagazzinamento dei dati (storage).
	Le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia devono essere collocate all'interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l'espletamento di specifiche mansioni) e munite di **dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi** delle persone ammesse, con indicazione dei relativi riferimenti temporali.
Incaricati del trattamento	Gli incaricati che accedono ai dati di traffico conservati per le finalità di cui all'art. 132 del Codice, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice medesimo, devono essere designati specificamente in rapporto ai dati medesimi.
Cancellazione dei dati	Allo scadere dei termini previsti dalle disposizioni vigenti, i dati di traffico sono resi non disponibili per le elaborazioni dei sistemi informativi e le relative consultazioni; sono altresì cancellati o resi anonimi senza alcun ritardo, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti, nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente, documentando tali operazioni al più tardi entro trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice.

I profili giuridici dei file di log

Principali misure ed accorgimenti per la conservazione dei dati di traffico per finalità di accertamento e prevenzione dei reati, prescritti dal Garante nel provvedimento del 17 gennaio 2008	
Altre misure (audit log)	**Devono essere adottate soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento**. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi database utilizzati.
Audit interno **Rapporti periodici**	La gestione dei dati di traffico per finalità di accertamento e repressione di reati deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati.

I profili giuridici dei file di log

Principali misure ed accorgimenti per la conservazione dei dati di traffico per finalità di accertamento e prevenzione dei reati, prescritti dal Garante nel provvedimento del 17 gennaio 2008	
Documentazione dei sistemi informativi	**I sistemi informativi utilizzati per il trattamento dei dati di traffico devono essere documentati in modo idoneo secondo i principi dell'ingegneria del software, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione**
Cifratura e protezione dei dati	**I dati di traffico trattati per esclusive finalità di giustizia vanno protetti con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema**. In particolare, devono essere adottate soluzioni che rendano le informazioni, residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei database o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche.

I profili giuridici dei file di log

- In questa sede è opportuno segnalare come la legge n. 48/2008 abbia introdotto nel Codice di Procedura Penale l'art. 254 bis relativo al Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni.
- Tale articolo stabilisce che "***l'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali***".

Il provvedimento del Garante sugli amministratori di sistema

- L'attività regolamentare del Garante ha da ultimo interessato un aspetto molto importante rispetto alla sicurezza informatica aziendale attraverso la previsione di alcune regole concernenti l'attività di amministratore di sistema ed in particolare l'obbligo di conservazione di alcune tipologie di file di log.

- Con il provvedimento del 27 novembre 2008 (pubblicato sulla Gazzetta Ufficiale lo scorso 24 dicembre) il Garante ha infatti prescritto specifiche misure ed accorgimenti ai titolari dei trattamenti (es. aziende) "*effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*"**.**

- In realtà il provvedimento non riguarda esclusivamente l'attività degli amministratori di sistema intesi tradizionalmente quali **soggetti che svolgono funzioni di gestione e manutenzione dei sistemi informatici** ma anche ad **altre categorie di figure professionali quali gli amministratori di banche dati, di reti e apparati di sicurezza e di sistemi di software complessi**, le cui attività possono comunque in determinati casi comportare dei rischi per la protezione dei dati personali.

Il provvedimento del Garante sugli amministratori di sistema

- Il Garante nel provvedimento ha in primo luogo specificato le ragioni che hanno reso necessaria la previsione di accorgimenti specifici per tali categorie professionali

- Viene in particolare rilevato che le attività di carattere tecnico svolte dagli amministratori di sistema, nell'ampia accezione sopra richiamata (es. backup dei dati, gestione dei supporti di memorizzazione, manutenzione dell'hardware), possono influire sulle informazioni conservate dall'azienda e le stesse attività, in queste circostanze, devono essere qualificate quali trattamenti di dati personali ai sensi del d.lgs 196/2003, ciò "*anche quando l'amministratore non consulti in chiaro le informazioni medesime*".

- La delicatezza del ruolo di questa figura professionale **è ulteriormente dimostrata, si legge nel provvedimento, dal fatto che il nostro legislatore in relazione ad alcune fattispecie di reato informatico** (es. accesso abusivo a sistema informatico, frode informatica, danneggiamento di informazioni, dati e programmi informatici) **ha previsto specifiche aggravanti in caso di loro commissione con abuso della qualità di amministratore di sistema**.

Il provvedimento del Garante sugli amministratori di sistema

- ***Per quanto rileva ai fini della trattazione del tema in esame, il provvedimento del Garante prevede che:***
  - Devono essere adottati **sistemi idonei alla registrazione degli accessi logici** (autenticazione informatica) **ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema**.
  - Le registrazioni (*access log*) devono avere **caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità** adeguate al **raggiungimento dello scopo per cui sono richieste**.
  - **Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi**.

Il provvedimento del Garante sugli amministratori di sistema

- **Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?**

  - **FAQ 9.** Per *access log* si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi *software*.

  - Gli *event records* generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (*timestamp*), una descrizione dell'evento (sistema di elaborazione o *software* utilizzato, se si tratti di un evento di *log-in*, di *log-out*, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato…).

Il provvedimento del Garante sugli amministratori di sistema

- **Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?**
  - **FAQ 10.** Qualora il sistema di *log* adottato generi una raccolta dati più ampia, **comunque non in contrasto con le disposizioni del Codice e con i principi della protezione dei dati personali**, il requisito del provvedimento è certamente soddisfatto.
  - **Comunque è sempre possibile effettuare un'estrazione o un filtraggio dei *logfiles* al fine di selezionare i soli dati pertinenti agli AdS.**

Il provvedimento del Garante sugli amministratori di sistema

- **Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?**
  - **FAQ 11.** La caratteristica di completezza è riferita all'insieme degli eventi censiti nel sistema di *log*, che deve comprendere tutti gli eventi di accesso interattivo che interessino gli amministratori di sistema su tutti i sistemi di elaborazione con cui vengono trattati, anche indirettamente, dati personali. L'analisi dei rischi aiuta a valutare l'adeguatezza delle misure di sicurezza in genere, e anche delle misure tecniche per garantire attendibilità ai *log* qui richiesti.

Il provvedimento del Garante sugli amministratori di sistema

- **Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?**
  - **FAQ 12. Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di *log* sono in genere disponibili nei più diffusi sistemi operativi**, o possono esservi agevolmente integrate con apposito *software*. **Il requisito può essere ragionevolmente soddisfatto con la strumentazione *software* in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di *log* su supporti di memorizzazione non riscrivibili**. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i *log server* centralizzati e "certificati".

  - **E' ben noto che il problema dell'attendibilità dei dati di *audit*, in genere, riguarda in primo luogo la effettiva generazione degli *auditable events* e, successivamente, la loro corretta registrazione e manutenzione**. Tuttavia il provvedimento del Garante non affronta questi aspetti, prevedendo soltanto, come forma minima di documentazione dell'uso di un sistema informativo, la generazione del *log* degli "accessi" (*log-in)* e la loro archiviazione per almeno sei mesi in condizioni di ragionevole sicurezza e con strumenti adatti, in base al contesto in cui avviene il trattamento, **senza alcuna pretesa di instaurare in modo generalizzato, e solo con le prescrizioni del provvedimento, un regime rigoroso di registrazione degli *usage data* dei sistemi informativi.**

Il provvedimento del Garante sugli amministratori di sistema

- **Quali sono esattamente gli obblighi e le modalità di conservazione dei log di accesso?**

  - **FAQ 13.** Non sono previsti livelli di robustezza specifici per la garanzia della integrità. La valutazione è lasciata al titolare, in base al contesto operativo (cfr. faq n. 14).

  - **FAQ 15**. **Il provvedimento non chiede in alcun modo che vengano registrati dati sull'attività interattiva (comandi impartiti, transazioni effettuate) degli amministratori di sistema.**

  - **FAQ 22. L'accesso a livello applicativo non rientra nel perimetro degli adeguamenti, in quanto l'accesso a una applicazione informatica è regolato tramite profili autorizzativi che disciplinano per tutti gli utenti i trattamenti consentiti sui dati.** L'accesso applicativo non è compreso tra le caratteristiche tipiche dell'amministratore di sistema e quindi non è necessario, in forza del provvedimento del Garante, sottoporlo a registrazione.

Il provvedimento del Garante sugli amministratori di sistema

- **Quali sono le finalità perseguibili nel controllo dei log?**
  - **FAQ 16.** La raccolta dei *log* serve per **verificare** anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso…). L'analisi dei *log* può essere compresa tra i criteri di valutazione dell'operato degli amministratori di sistema.

La computer forensics aziendale

La computer forensics aziendale

- La definizione sopra delineata di digital forensics è legata prevalentemente ad un ambito “legale” o “processuale” della acquisizione, dell’analisi e della presentazione delle evidenze informatiche.
- Uno studio di alcuni esperti della Sun Microsystems (Weise, Powell “*Using Computer Forensics When Investigating System Attacks”*) definisce la computer forensics aziendale come l’attività che consiste **nel catturare, processare, preservare e analizzare le informazioni ottenute da un sistema, da una rete (network), da un’applicazione o da un’altra risorsa informatica, per determinare la fonte di un attacco a quelle risorse**.
- In base al medesimo studio gli obiettivi principali della computer forensics aziendale sono:
  - aiutare gli interessati a stabilire quale evento indesiderabile è avvenuto, se è avvenuto;
  - recuperare, processare, memorizzare e preservare elementi di prova per supportare il perseguimento del colpevole, nel caso vi sia l’interesse di farlo;
  - usare la conoscenza acquisita per prevenire il verificarsi di ulteriori casi simili;
  - determinare la motivazione e gli scopi degli attaccanti.

La computer forensics aziendale

- Gli esiti delle investigazioni effettuate dall'azienda hanno dunque, almeno in una prima fase una rilevanza esclusivamente interna, ma possono comunque costituire il presupposto per eventuali successive azioni legali.
- In considerazione dell'eventuale rilevanza esterna delle attività di indagine effettuate a livello aziendale mirate alla ricerca e analisi di evidenze informatiche, le stesse devono essere poste in essere utilizzando le metodologie proprie della computer forensics (ovvero quelle generalmente utilizzate a fini processuali).

La computer forensics aziendale

- Come rilevato dalla dottrina (cfr. Luparia – Ziccardi, Investigazione penale e tecnologia informatica, Giuffrè, 2008) "*I fini delle due forensics sono, però, sovente gli stessi: scoprire un determinato fatto, le sue prove, i collegamenti ad uno o più soggetti, valutare se tale fatto è nocivo o meno ed elaborare dei metodi correttivi per arrivare a tali fini*".

Le linee guida del Garante

- Oggi non esiste una normativa specifica che disciplini la possibilità o meno di navigare in Internet da parte del dipendente, né che fissi chiaramente quali sono i poteri di controllo e repressione da parte del datore di lavoro dei comportamenti illeciti
- Occorre quindi valutare quali normative si possono considerare applicabili e in quali limiti
- Le due normative che occorre tenere in considerazione quando si analizzano le tematiche dei controlli sono:
  - il d.lgs 196/03, che disciplina il trattamento dei dati e quindi in linea generale i diritti di riservatezza in capo (anche) ai lavoratori
  - la legge 300 del 1970, meglio nota come Statuto dei Lavoratori
- Occorre inoltre considerare l'art. 616 c.p. in base al quale:
  - Chiunque prende cognizione del contenuto di una corrispondenza chiusa a lui non diretta è punito… *omissis*
  - Per "corrispondenza" si intende quella epistolare, telegrafica, telefonica Per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza

Le linee guida del Garante

- la normativa in materia di trattamento dei dati incide nella tematica inerente il controllo sui lavoratori in quanto le informazioni relative alla navigazione (ora di collegamento, tempo di collegamento, siti visitati ecc.) sono dati personali sottoposti alla regolamentazione di cui al d.lgs 196/03

- **L'articolo 4 dello Statuto dei Lavoratori stabilisce che**
  - E' vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori

  - Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali

Le linee guida del Garante

- **I c.d. "*controlli difensivi*":**
  - Con l'esplosione della tecnologia informatica hanno assunto particolare rilievo i "controlli difensivi", cioè quei controlli tesi alla protezione di beni costituzionalmente garantiti (proprietà e salute)
  - Il problema è che spesso, le apparecchiature tese al controllo dei beni indirettamente permettono altresì il controllo della prestazione lavorativa

Le linee guida del Garante

- Il Garante privacy, con il provvedimento generale del 1 marzo 2007, ha fornito concrete indicazioni in ordine all'uso dei computer sul luogo di lavoro
- Secondo il Garante dall'analisi dei siti web visitati si possono trarre informazioni anche sensibili sui dipendenti e i messaggi di posta elettronica possono avere contenuti a carattere privato
- Occorre dunque prevenire usi arbitrari degli strumenti informatici aziendali e la lesione della riservatezza dei lavoratori

Le linee guida del Garante

Le linee guida del Garante: principi generali

- **Principio di *necessità***
  - i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (*art. 3 del Codice*)

- **Principio di *correttezza***
  - le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (*art. 11, comma 1, lett. a), del Codice*). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati

- **Principio di *pertinenza* e di *non eccedenza***
  - i trattamenti devono essere effettuati per finalità *determinate*, *esplicite* e *legittime* (*art. 11, comma 1, lett. b), del Codice)*. Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"*

Le linee guida del Garante

Le linee guida del Garante: controlli e correttezza nel trattamento

- **Disciplina interna**
  - Il datore di lavoro ha l'onere di indicare, chiaramente e in modo particolareggiato, **quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli**
  - Il datore di lavoro deve tenere conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali

Le linee guida del Garante

Le linee guida del Garante: controlli e correttezza nel trattamento

- **A seconda dei casi andrebbe ad esempio specificato:**
  - Gli eventuali comportamenti che non sono tollerati rispetto alla "navigazione" in Internet oppure alla tenuta di file nella rete interna
  - La possibilità o meno di utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo
  - **Quali informazioni sono memorizzate temporaneamente** (ad es., le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente

Le linee guida del Garante

Le linee guida del Garante: Controlli e correttezza nel trattamento

- **A seconda dei casi andrebbe ad esempio specificato:**
  - Se e **quali informazioni sono eventualmente conservate per un periodo più lungo**, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*)
  - Se, e in quale misura, il datore di lavoro si riserva di **effettuare controlli in conformità alla legge**, anche saltuari o occasionali, indicando le ragioni legittime – specifiche e non generiche – per cui verrebbero effettuati e le relative modalità
  - Suali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente

Le linee guida del Garante

Le linee guida del Garante Controlli e correttezza nel trattamento

- **A seconda dei casi andrebbe ad esempio specificato:**
  - Le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento **all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti**
  - Se sono utilizzabili **modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato**
  - Quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato **l'eventuale segreto professionale** cui siano tenute specifiche figure professionali
  - Le prescrizioni interne sulla sicurezza dei dati e dei sistemi (*art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10*)

Le linee guida del Garante

Le linee guida del Garante Controlli e correttezza nel trattamento

- **Informativa (art. 13 del Codice)**
  - 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
  - Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli

Le linee guida del Garante

Le linee guida del Garante: apparecchiature preordinate al controllo a distanza

- Il trattamento dei dati che ne consegue è **illecito**, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli

- Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro

- A parte eventuali responsabilità civili e penali, **i dati** trattati illecitamente **non sono utilizzabili** (art. 11, comma 2, del Codice)

Le linee guida del Garante

Le linee guida del Garante: Apparecchiature preordinate al controllo a distanza

- In particolare non 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. É il caso, ad esempio:
  - della lettura e della 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
  - della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore
  - della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo
  - dell'analisi occulta di computer portatili affidati in uso

Le linee guida del Garante

Le linee guida del Garante:programmi che consentono controlli "indiretti"

- Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), **di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò, anche in presenza di attività di controllo discontinue**

- Il trattamento di dati che ne consegue può risultare **lecito**. Resta ferma la necessità di **rispettare 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 controllare i movimenti o la produttività dei lavoratori

Le Linee guida del Garante: i principi di pertinenza e non eccedenza dei controlli

- Graduazione dei controlli
  - Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata
  - L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza
  - 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

Le Linee guida del Garante: i principi di pertinenza e non eccedenza dei controlli

- Graduazione dei controlli
  - Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree
  - Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale
  - Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati

Le Linee guida del Garante: i principi di pertinenza e non eccedenza dei controlli

- Conservazione
  - I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria
  - In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario (e predeterminato) a raggiungerla

Le Linee guida del Garante: i principi di pertinenza e non eccedenza dei controlli

- Conservazione
  - Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:
    - 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
    - all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria
  - In questi casi, il trattamento dei dati personali deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati

Le Linee guida del Garante - Presupposti di liceità del trattamento: bilanciamento di interessi

- Datori di lavoro privati
  - I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (*v., in particolare, art. 4, secondo comma, dello Statuto*), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili
  - Ciò, può avvenire:

    se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (*art. 24, comma 1, lett. f) del Codice*)

    in caso di valida manifestazione di un libero consenso

    anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi (*art. 24, comma 1, lett. g), del Codice*)

Le Linee guida del Garante - Presupposti di liceità del trattamento: bilanciamento di interessi

- Datori di lavoro privati
  - Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro)
  - L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26)

Le Linee guida del Garante. Individuazione dei soggetti preposti

- Il datore di lavoro può ritenere utile la designazione (facoltativa), specie in strutture articolate, di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità (*art. 29 del Codice*)
- Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti
- Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa
- Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni

Le linee guida del Garante

- **Il datore di lavoro può controllare la casella di posta elettronica aziendale del dipendente?**
  - Le linee guida chiariscono che, in assenza di un'adeguata policy, che stabilisca l'uso esclusivamente aziendale della e-mail assegnata al dipendente, quest'ultimo (o i terzi) può legittimamente aspettarsi la confidenzialità della stessa
  - Sembra quindi che in assenza di una policy e di un'idonea informativa i controlli posti in essere sulla casella del dipendente siano illegittimi con il rischio di violazione dell'articolo 616 c.p.
  - Anche in presenza di una policy, comunque, i controlli non devono violare i principi di pertinenza e non eccedenza
  - Si consideri inoltre che l'allegato B del d.lgs 196/2003 prevede che "*Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite* ***idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema****. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato*"

Analisi delle Linee Guida

- Come devono essere considerati i controlli difensivi?
  - Le linee guida sembrano orientate a considerare i controlli difensivi come sottoposti all'applicazione dell'articolo 4 comma 2 dello Statuto dei Lavoratori, aderendo all'orientamento maggioritario della giurisprudenza
  - Parte della dottrina è orientata a considerare sottoposti all'applicazione dell'articolo 4 comma 2 dello Statuto dei Lavoratori solo i controlli "ex ante" (in via preventiva) e non quelli "ex post" (reazione posta in essere per fronteggiare un illecito)
  - Al momento, vista l'incertezza in materia, la soluzione consigliabile è il raggiungimento di un accordo con le rappresentanze sindacali anche con riferimento ai controlli difensivi ex post

Come costruire una policy aziendale

Suggerimenti delle Linee Guida per la costruzione delle policy
Indicare se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il download di software o di file musicali), oppure alla tenuta di file nella rete interna
Indicare in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di webmail, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro)
Specificare quali informazioni sono memorizzate temporaneamente (ad es., le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente
Indicare se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log)

Come costruire una policy aziendale

Suggerimenti delle Linee Guida per la costruzione delle policy
Specificare se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime, specifiche e non generiche per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni)
Indicare quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente
Elencare le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;

Come costruire una policy aziendale

Suggerimenti delle Linee Guida per la costruzione delle policy
Specificare se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato
Indicare quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali
Elencare le prescrizioni interne sulla sicurezza dei dati e dei sistemi

Analisi di alcune linee guida per le attività di computer forensics aziendale

Le linee guida di Sun Microsystem

- Nello studio della SUN cui si è fatto cenno, vengono fornite alcune linee guida specifiche per la gestione di investigazioni di forensics in ambito aziendale.
- Il documento presenta alcune definizioni preliminari:
  - **Attacco**: qualsiasi tipo di attività dannosa effettuata contro risorse informatiche aziendali, inclusi gli accessi non autorizzati, la diffusione di virus , l'alterazione o la distruzione di dati o gli attacchi di tipo "denial of service"
  - **Prova**: è definita come qualunque informazione fisica o elettronica (quali documentazione scritta o elettronica, file di log, dati, report, hardware, software, immagini di disco, ecc) che è raccolta durante un'investigazione di forensics aziendale. La prova include sia file generati da computer (es. file di log) che file prodotti da esseri umani (es. fogli di calcolo, documenti, messaggi di posta elettronica). Lo scopo di raccogliere una prova è quello di

    determinare la provenienza di un attacco

    evidenziare tutti i danni provocati da un attacco

    introdurla all'interno di un eventuale processo

    A tal fine la prova deve essere ammissibile in un tribunale ed essere dunque in grado di resistere a contestazioni circa la sua integrità e autenticità

Le linee guida di Sun Microsystem – Principi chiave per le "computer forensics investigation"

- Durante l'acquisizione e l'analisi delle evidenze informatiche, gli investigatori devono essere consapevoli degli aspetti legali delle loro azioni
- In caso di attacco, l'azienda deve decidere se intende perseguire o meno l'attaccante

  La decisione di intraprendere azioni legali può comportare sacrifici aggiuntivi sia in termini di tempo che di sforzi dal momento che è necessario adottare le misure necessarie per preservare adeguatamente le immagini dei computer e i dati affinché gli stessi possano essere ammessi come prove in un tribunale.

  Se l'organizzazione è assolutamente certa di non voler perseguire l'attaccante alcune misure potrebbero non essere necessarie (per gli esperti di SUN è comunque preferibile, anche in questi casi, trattare le evidenze raccolte come se si dovesse successivamente produrle in un tribunale)

Le linee guida di Sun Microsystem – La corretta gestione delle evidenze informatiche

- Secondo lo studio di Sun una parte importante di ogni investigazione di forensics è il modo in cui le evidenze sono raccolte e preservate al fine di supportare un'azione legale in un tribunale. Occorre quindi
- **Autenticità:**
  - quando si maneggia una prova l'obiettivo è quello di assicurare che, nel caso fosse contestata, si possa dimostrare che la stessa è autentica e non modificata ovvero che:

    Proviene dal sistema attaccato

    Rappresenta accuratamente lo stato del sistema in un dato momento
  - Lo standard di autenticità richiede che le registrazioni del computer non siano stati alterati, cancellati o alterati dopo la loro creazione.
- **Affidabilità:**
  - l'affidabilità di un record di un computer dipende da quella del sistema informatico oggetto di investigazione
  - Se viene dimostrato che un sistema è affidabile e non corrotto, allora i record prodotti da quel sistema si possono considerare ragionevolmente come autentici e ammissibili come prove

Le linee guida di Sun Microsystem – La corretta gestione delle evidenze informatiche

- **Catena di custodia**
  - nel corso dell'esecuzione di un'investigazione di forensics, tracciare la catena di custodia è essenziale per preparare la prova per un eventuale azione legale nei confronti dell'attaccante e per mitigare le possibili contestazioni durante un eventuale processo. **La catena di custodia è definita come un sistema per mantenere e documentare, nel dettaglio, la storia cronologica dell'investigazione, inclusa la raccolta , gestione e preservazione della prova, insieme ad un record di chiunque sia venuto in contatto con la stessa**.
  - Una catena di custodia deve dimostrare che la prova è stata raccolta dal sistema in questione, e che è stata immagazzinata e gestita senza alterazioni.

Le linee guida di Sun Microsystem – Mantenere intatto il sistema originale

- Nel corso di un'investigazione di computer forensics è necessario mantenere l'integrità del sistema informatico originale creando un immagine dello stessi. Occorre quindi:
  - Fare una copia del sistema compromesso

    creare due copie precise e complete dell'immagine del disco e del memory dump (una copia deve essere prodotta come fonte di prova, l'altra deve essere usata per l'analisi)

    in nessun caso l'investigazione dovrebbe essere condotta sul sistema originale o sulla copia utilizzata a fini probatori

    gli investigatori per creare copie delle immagini del sistema devono utilizzare strumenti che consentano di disabilitare la possibilità di scrivere o cambiare i dati esistenti
  - Firmare i dati attraverso tecniche crittografiche

    Viene raccomandato agli investigatori di generare una firma basata su crittografia e/o l'hash dell'immagine originale del sistema per dimostrare che l'immagine non è stata modificata.
  - Assicurare fisicamente i dati

Le linee guida di Sun Microsystem

- Nello studio di Sun Microsystem, prima di iniziare un'investigazione di computer forensics aziendale (in presenza di un attacco o di un fatto sospetto) occorre affrontare tutta una serie di questioni preliminari:
  - Esiste un collegamento tra i dati e le azioni di un hacker o di un altro soggetto?
  - Quali sono i possibili profili di responsabilità in capo all'azienda che sospetta che i suoi dati possano essere stati compromessi?
  - In quale momento occorrerebbe avvertire gli altri soggetti o società che potrebbero essere danneggiati dall'eventuale intrusione?
  - In che momento è necessario dare avvio ad azioni legali?
  - Esistono dati (di particolare rilevanza) che devono essere diffusi come parte della prova e che potrebbero avere effetti negativi sulla società?
  - Il sistema è stato realmente oggetto di un attacco? O si tratta semplicemente di problemi di performance, difetti di configurazione e/o di programmazione?

Le linee guida di Sun Microsystem

- Per garantire una corretta analisi di computer forensics occorre inoltre prendere in considerazione queste 4 regole fondamentali:
  - Non farsi prendere dal panico
  - Trattare qualsiasi elemento come se fosse una possibile prova
  - Elaborare un piano per gestire la situazione
  - Isolare il sistema

La giurisprudenza rilevante

- In materia di sequestro probatorio una recente sentenza della Corte di Cassazione ha stabilito che: "*In un'inchiesta per concorrenza sleale è illegittimo il sequestro dell'intero server aziendale e di altri documenti cartacei che non abbiano attinenza con i progetti, il know-how o comunque con i reati contestati, in quanto non sussiste nella specie il vincolo di pertinenzialità tra tutti i beni sequestrati e le ipotesi di reato configurate" (sent. n. 12107/2008)*

La giurisprudenza rilevante

- il Tribunale di Milano (sentenza dell'11 marzo 2005) ha invece stabilito che "è legittima la convalida del sequestro dell'hard disk che contiene dati rilevanti in ordine alla gestione di un database, in quanto il **provvedimento è finalizzato ad assicurare i mezzi di prova in ordine ai reati per cui si procede** anche se ciò avviene in sede di indagini sollecitate dalla difesa dopo la conclusione delle indagini preliminari. Il vincolo reale sull'HD è necessario e finalizzato a preservare il bene e consentire un utile esame dei dati ivi contenuti".
  - Si aggiunga che il sequestro del supporto non è di per sé sufficiente a garantire la successiva genuinità delle tracce informatiche riscontrate.
  - Occorre infatti che l'attività di accertamento sul supporto sequestrato sia effettuata su immagini dello stesso posto che altrimenti si avrebbe come risultato quello di alterare il reperto e di rendere quindi inutilizzabili le informazioni dallo stesso ricavate.
  - Il compimento di accertamenti non ripetibili in sede penale comporta infatti il **diritto dei difensori delle parti coinvolte di assistervi** anche a mezzo di propri consulenti, a pena di inutilizzabilità degli accertamenti medesimi

La giurisprudenza rilevante

- Sempre in materia di sequestro, il Tribunale di Brescia (sentenza del 9 ottobre 2006) ha stabilito che "*Il sequestro di un hard-disk per finalità esplorative sorrette dalla sola ipotesi investigativa del Pubblico Ministero non è ammissibile nei confronti di una persona non sospettata dalla commissione di alcun reato . Il sequestro di un intero hard,-disk consente certamente l'acquisizione di elementi probatori, ma implica anche l'acquisizione di dati che esulano dal contesto per il quale l'atto è disposto. Tale genere di sequestro esige un ambito di corretta e ristretta operatività per evitare connotazioni di spropositata afflittività e di lesione di beni costituzionalmente protetti.*"

La giurisprudenza rilevante

- In riferimento a quanto esposto circa i profili giuridici dei file di log, la sentenza del Tribunale di Chieti (30 maggio 2006) afferma che “le attività di apprensione dei ‘file di log’ da parte della polizia giudiziaria devono essere accompagnate da un attento controllo circa le modalità di conservazione dei dati informatici, allo scopo di verificare l’assenza di manipolazioni e la conseguente genuinità delle evidenze digitali. In mancanza di tali adempimenti i ‘file di log’, specie ove provengano dalla stessa persona offesa, costituiscono materiale del tutto insufficiente a fondare qualsivoglia affermazione di responsabilità al di là del ragionevole dubbio”
  - Tale orientamento ha trovato conferma nell’appena sopra richiamato nuovo articolo 254 bis relativo al *Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni. In base all’articolo in esame l’acquisizione,* per esempio, di file di log presso i fornitori deve avvenire “. *mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità”.*
  - È evidente che il mancato utilizzo di tali procedure comporterebbe l’inutilizzabilità dei dati diversamente raccolti.

La giurisprudenza rilevante

- Il Tribunale di Bologna (sentenza del 22 dicembre 2005) ha stabilito che "dal compimento di investigazioni informatiche che si discostano dalla migliore pratica scientifica non discende un'automatica inutilizzabilità del materiale raccolto. Spetta infatti alla difesa l'onere di dimostrare in che modo la metodologia utilizzata ha concretamente alterato i dati ottenuti". I risultati cui conduce un metodo non conforme alla migliore pratica scientifica utilizzato dalla polizia giudiziaria, secondo la citata sentenza, sarebbero liberamente valutabili dal giudice (in applicazione del principio di cui all'articolo 192 c.p.p.) alla luce del contesto probatorio complessivo.
  - Si tratta di una tesi che, come già sopra detto, non si ritiene condivisibile in quanto da un lato il giudice deve verificare la validità scientifica dei criteri e dei metodi d'indagine per stabilire la loro affidabilità in sede processuale e, dall'altro, è onere delle autorità inquirenti utilizzare metodologie che garantiscano l'integrità della prova
  - Si rimanda a quanto detto in precedenza in relazione alle rilevanti modifiche introdotte dalla legge n. 48/2008 e in particolare agli artt. 244 c.p.p. (ispezioni) e 247 c.p.p. (perquisizioni)..

I problemi aperti

- Gli organi inquirenti, adottano spesso differenti metodologie di computer forensics (alcune volte costituite dalla passiva adozione di guidelines di paesi stranieri che mal si adattano al panorama giuridico italiano) ostacolando in questo modo l'attività di interpretazione in sede giudiziale.

I problemi aperti

- Le problematiche sopra riscontrate erano in parte dovute all'assenza di una legislazione che definisse le regole da osservare per l'acquisizione e conservazione delle prove informatiche, regole che consentissero agli operatori di affrontare le attività di indagine all'interno di un preciso contesto normativo e che fornissero ai giudici gli strumenti per valutare con maggiore sicurezza la validità delle metodologie utilizzate.
- Nel contesto penale, le modifiche e integrazioni apportate dalla legge 48/2008 al Codice di Procedura Penale dovrebbero consentire nel tempo la risoluzione delle problematiche sopra evidenziate, dal momento che stabiliscono, come visto, in relazione, per esempio, alle attività di ispezione e perquisizione l' obbligo per la l'autorità giudiziaria di adottare "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".
- Tale obbligo avrà come diretta conseguenza la necessità di stabilire quali siano i sistemi idonei a raggiungere il risultato voluto da tali norme nonché di creare regole tecniche chiare per l'esecuzione delle operazioni

I problemi aperti

La Computer Forensics a livello aziendale

- Troppo sovente le aziende preferiscono non denunciare gli attacchi informatici subiti per il timore di vedere danneggiata la propria immagine.

- Dotarsi degli strumenti per reagire a tali attacchi e per supportare l'autorità giudiziaria nell'effettuazione delle investigazioni al fine di individuare il responsabile appare invece la via preferibile.

- Le competenze necessarie all'applicazione delle metodologie di Computer Forensics all'interno delle aziende richiedono un grosso sforzo economico e organizzativo, forse al momento affrontabile solo dalle aziende di grandi dimensioni.

- La creazione di procedure sia pur non a livello avanzato da adottare in caso di attacco ai fini della preservazione delle prove informatiche possono essere, comunque, di sicuro supporto alle indagini dell'autorità giudiziaria ed evitano che l'attività di indagine sia vanificata dall'inquinamento delle prove proprio a opera del soggetto leso dall'attività criminosa.