PROCURA DELLA REPUBBLICA

PRESSO IL TRIBUNALE DI SIRACUSA

I provvedimenti cautelari reali in materia di indagini informatiche

Antonio Nicastro
Sost. Procuratore della Repubblica

Premessa.

Nella società contemporanea il computer è diventato assoluto protagonista della nostra vita, ad esso affidiamo il nostro lavoro, i nostri ricordi, attraverso la rete ci informiamo, aggiorniamo le nostre conoscenze, comunichiamo, relazioniamo con il prossimo, effettuiamo transazioni commerciali, consultiamo il nostro conto in banca, attuiamo una serie di rapporti "on-line" che vanno acquisendo sempre maggiori spazi nella dinamica sociale di ognuno di noi.

Tuttavia la navigazione in rete e le svariate possibilità che lo strumento informatico offre, la possibilità di assumere un'identità virtuale che si accompagna sovente ad una sensazione diffusa di anonimato, costituiscono evenienze che prestano il fianco alla commissione di vecchi e nuovi reati.

Alla luce di questa evoluzione del fenomeno, corrisponde una produzione normativa-regolamentare sempre più copiosa, ma non sempre al passo con i tempi.

I comportamenti che in internet costituiscono violazioni alla legge penale sono, infatti, molteplici ed in genere vengono distinti a seconda dell'oggetto dell'azione criminale:

- reati concepibili solo ai danni di un computer o di una rete telematica;

- reati comuni commessi attraverso la rete internet

A titolo esemplificativo si segnalano alcuni tra i possibili reati realizzabili attraverso la rete:

- **Accesso abusivo ad un sistema informatico o telematico**[1] (art. 615-ter codice penale). Il reato punisce con la reclusione fino a 3 anni (da 1 a 5 anni nelle ipotesi aggravate) l'introduzione abusiva di un soggetto in un sistema informatico protetto da misure di sicurezza (per esempio: password d'accesso) ovvero colui che si trattiene all'interno del sistema contro la volontà espressa o tacita di chi ha diritto di escluderlo. Non rilevano le

[1] Norma introdotta dall'art. 4 legge 547/1993.

finalità dell'accesso: viene punito anche se avviene per gioco e non ci sono danneggiamenti al sistema violato. Se l'accesso causa un danno al sistema (o ai dati in esso custoditi ovvero determina l'interruzione totale o parziale del suo funzionamento) la pena è della reclusione da 1 a 5 anni (da 3 a 8 anni se il sistema è di interesse pubblico).
Attraverso tale norma il legislatore ha assicurato la protezione del c.d. "**domicilio informatico"** quale spazio ideale (ma anche fisico) in cui sono contenuti i dati informatici di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene costituzionalmente protetto. Tuttavia l'art. 615 ter non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concretizza nello *jus exludendi alios,* quale che sia il contenuto dei dati informatici racchiusi in esso, purchè attinenti alla sfera di pensiero, all'attività, lavorativa e non, dell'utente; con la conseguenza che la tutela legale si estende anche agli aspetti economico patrimoniali dei dati sia che il titolare dello jus excludendi sia persona fisica , sia giuridica, pubblica o privata, o altro ente. [2]

- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici**[3] (art. 615 quater c.p.). Il reato sanziona l'acquisizione, la riproduzione, la diffusione, la comunicazione o la consegna di codici di accesso (password) o altri mezzi idonei (anche meccanici) all'accesso ad un sistema informatico. Oggetto di sanzione anche il fornire indicazioni o istruzioni utili all'accesso (per esempio, le istruzioni per ricostruire una parola chiave). Il reato si configura solo se il soggetto agisce per procurare a sé o ad altri un profitto (cioè un vantaggio patrimoniale, ma non necessariamente un guadagno) o di arrecare un danno ad altri.
Trattasi di reato di pericolo: la condotta è prodromica rispetto ad altre condotte delittuose che possono consumarsi una volta superato l'ostacolo delle misure di protezione

- **La diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico**[4] (art. 615 quinquies c.p.) Il reato sanziona chi 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 favorirne 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.**
Il legislatore, prevedendo una condotta il più possibile variegata finalizzata alla tutela di sistemi informatici o delle informazioni in essi contenute, onde sanzionare chi

[2] Cfr. Cass. 4.10.1999, ced cass n. 214946
[3] Norma introdotta dall'art. 4 legge 547/1993.
[4] Norma introdotta dall'art. 4 legge 547/1993 e radicalmente novellata con la legge 18.3.2008 n. 48

agisca allo scopo di danneggiare o alterare l'hardware, il software , i dati e le informazioni contenute in un sistema informatico o telematico.

- **L'intercettazione abusiva di comunicazioni telematiche**[5] (art. 617 quater c.p.). Il reato sanziona chiunque fraudolentemente intercetta, impedisce o interrompe comunicazioni informatiche o telematiche. La norma contiene poi una seconda ipotesi volta a sanzionare la condotta di chi, acquisito il contenuto di una comunicazione lo rivela, con qualsiasi mezzo di informazione al pubblico, ad altri. In questa seconda ipotesi, si costituisce un'ipotesi di reato diversa da quella di cui al comma 1 e non necessariamente concorrente.
Il legislatore mira a tutelare non solo la riservatezza, ma anche la regolarità delle comunicazioni, che, nei limiti di legge, si vogliono libere, complete e senza interruzioni.

- **Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche e/o telematichere**[6] (art. 617 quinquies c.p.)
La fattispecie sanziona la condotta chiunque installa apparecchiature "atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi". Non vi sono dubbi che tale norma sanzioni l'installazione abusiva di programmi in grado di individuare e memorizzare i tasti premuti dall'utente sul computer (keylogger) nonché la predisposizione di programmi in grado di intercettare i pacchetti in transito attraverso una rete acquisendone i contenuti e permettendo all'utente di visualizzarli (sniffer).

- **Falsificazione, alterazione o soppressione di comunicazioni informatiche o telematiche**[7] (art. 617 sexies c.p.) La norma sanziona la condotta posta in essere da chiunque, al fine di arrecare a sé o ad altri un vantaggio o di arrecare ad altri un danno, formi falsamente ovvero alteri o sopprima, in tutto o in parte, il contenuto di una comunicazione informatica o telematica. Il reato è caratterizzato dalla tutela del contenuto della comunicazione e si consuma nel momento in cui viene utilizzato (falsificato, alterato o soppresso) il testo intercettato.

- **Frode informatica** (art. 640 ter c.p.)[8] Il reato di frode informatica (art. 640-ter) prevede che un soggetto, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procuri a sé o ad altri un ingiusto profitto con altrui danno .
Il delitto de quo ha la medesima struttura e presenta i medesimi elementi costitutivi del delitto di truffa, dal quale si differenzia solamente per il fatto che l'attività fraudolenta dell'agente investe non la persona (soggetto passivo) di cui difetta

[5] Norma introdotta dall'art. 6 legge 547/1993.
[6] Norma introdotta dall'art. 6 legge 547/1993.
[7] Norma introdotta dall'art. 6 legge 547/1993.
[8] Norma introdotta dall'art. 10 legge 547/1993.

l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.

L'esame delle fattispecie non contempla le ipotesi di cui agli artt. 600 ter e ss c.p., oggetto di altra relazione.

La legge 18 marzo 2008 n. 498 ha introdotto nel codice penale alcune novità importanti, che appare opportuno esaminare:

Articolo 635-bis. – **Danneggiamento di informazioni, dati e programmi informatici**. – 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. 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".

L'articolo si ricollega, non senza una certa tautologia, al nuovo 635-quater:

"Articolo 635-quater. – **Danneggiamento di sistemi informatici o telematici**. – 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. 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."

Sono abrogati il secondo ed il terzo comma dell'articolo 420 del codice penale mentre, per contrastare **i crimini informatici che colpiscano lo Stato, enti pubblici o comunque di pubblica utilità**, è introdotto:

Articolo 635-ter. – **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità**. – 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.
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."

Articolo 635-quinquies. – **Danneggiamento di sistemi informatici o telematici di pubblica utilità**. – Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. 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 evidenziate interrelazioni tra crimine e tecnologia informatica, devono necessariamente condurci attraverso l'esame degli strumenti di cui l'investigatore può far uso per l'identificazione degli autori del reato e l'acquisizione degli elementi di prova processualmente utilizzabili.

La tematica dell'incontro pone necessariamente in evidenza la funzione assolutamente preminente del **sequestro probatorio,** istituto che a differenza del sequestro preventivo, non è una misura cautelare reale bensì un mezzo di ricerca della prova, e comporta l'imposizione di un vincolo di temporanea indisponibilità sulla res che può essere imposto soltanto **ai beni qualificabili come corpo di reato o cose pertinenti al reato.**

La nozione di corpo di reato, definito dalla norma (art. 253 c.p.p.) con una dizione che ripete quella relativa alla confisca (art. 240 c.p.) comprende i ***corpora delicti*** **ed i** ***producta sceleris*** , cioè cose che siano in rapporto diretto ed immediato con l'azione delittuosa.

La nozione di cose pertinenti al reato, invece, è necessariamente generica, in quanto comprende tutte quelle cose che si trovino in rapporto indiretto con la fattispecie concreta e sono strumentali, secondo i principi della libera prova e del libero convincimento del giudice, all'accertamento dei fatti. In tale dizione vanno quindi ricomprese *le cose necessarie sia alla dimostrazione del reato e delle modalità di preparazione*

ed esecuzione, sia alla conservazione delle tracce, all'identificazione del colpevole,all'accertamento del movente ed alla determinazione dell'ante factum e del post factum, comunque ricollegabili al reato, pur se esterni all'iter criminis, purchè funzionali alla finalità perseguita, cioè all'accertamento del fatto ed all'identificazione dell'autore.

Come evidenziato in premessa, la pervasività della tecnologia informatica ha comportato, tra l'altro, un sensibile aumento dei casi in cui i computer e gli apparati di comunicazione digitali vengono utilizzati come mezzo per commettere reati con la concreta possibilità che tali apparati in memoria conservino le prove della commissione dell'illecito (ed identificazione dell'autore) , e spesso si tratta di reati non prettamente informatici. Gli elementi idonei ad accertare il reato, le c.d. prove, sono costituiti da files contenuti nei vari tipi di supporti di memorizzazione, dai comuni hard disk, CD/DVD, floppy, USB pen drive, fino ai molteplici tipi di memory card, nastri magnetici, smart card ecc. Si parla pertanto di ***prove digitali[9], di impronte elettroniche da ricercare e da analizzare.[10]***

Le particolarità intrinseche di questi strumenti, in quanto corpo del reato o cose pertinenti al reato, nel senso sopra evidenziato, comportano una serie di approfondimenti sia da un punto di vista squisitamente tecnico, che da un punto di vista giuridico. I due aspetti non possono essere isolatamente affrontati, atteso che è sempre più necessario modellare lo strumento giuridico alle caratteristiche tecniche dell'elemento di prova da ricercare.

---

[9] La definizione più condivisa in dottrina di prova digitale individua con detto termine qualsiasi informazione, avente valore probatorio, che sia memorizzata o trasmessa in formato digitale

[10] Occorre non confondere il concetto di prova digitale con quello di documento informatico. Quest'ultimo trovava definizione nel previgente articolo 491 bis c.p. che indicava quale documento informatico qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli. Tale definizione è stata soppressa dalla Legge 48/2008. tale modifica ha sganciato il concetto di documento da quello del supporto. Il se5rvizio studi della Camera dei Deputati sul punto evidenzia che l'equiparazione tra documento e supporto rischia di apparire in qualche misura fuorviante perché attribuisce al documento informatico una pretesa dimensione materiale da cui esso, a ben vedere, proprio per le intime caratteristiche, prescinde. Ciò premesso il documento informatico secondo questa chiave di lettura altro non è che una rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti ma, può non assumere rilevanza probatoria se non sottoscritto con firma elettronica con certificato.
Deve distinguersi tra documento sottoscritto con firma elettronica semplice liberamente valutabile in giudizio, in considerazione delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità – oggetto di accertamento da parte del giudice – mentre il documento informatico sottoscritto con firma digitale qualificata ha la valenza di scrittura privata.
La Legge 48/2008 ha introdotto il nuovo delitto di cui all'art. 495 bis che sanziona la falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità propria o di altri.

Si pone infatti, quanto meno, un duplice ordine di problemi: quello relativo alle modalità tecniche di acquisizione, trattamento e custodia delle prove che risiedono in memorie di massa, e quello inerente gli strumenti giuridici più opportuni che la procedura penale mette a disposizione per la ricerca della prova, tenendo conto dei diritti e delle garanzie dell'indagato.

Tale esigenza si avverte non solo per garantire una corretta acquisizione degli elementi di prova da spendere in dibattimento, ma anche per operare un approccio corretto con il dato acquisito, in modo tale che esso non possa essere ripudiato, a garanzia di una genuina valutazione, sin dalle primissime fasi delle indagini preliminari, delle posizioni dei soggetti indagati (e di eventuali persone offese) e degli elementi di prova acquisiti a loro carico o a loro favore.

Tecnicamente, si può osservare che i *dati memorizzati su hard disk o qualunque altro supporto riscrivibile sono per loro natura facilmente alterabili, danneggiabili, e ciò proprio a cagione della loro intrinseca fragilità.*

Occorre da un lato evitare modifiche al supporto "originale" e dall'altro garantire in ogni momento la perfetta identità tra i dati presenti nel supporto in sequestro e la copia da utilizzare per gli accertamenti.

La stessa distinzione tra originale e copia perde il senso che assume nella riproduzione ad esempio di documenti cartacei, dato che una sequenza di bit scritta con identico ordine e posizione su due memorie digitali non presenta alcuna differenza.

Trattandosi di cose immateriali, i files contenenti prove del reato devono essere necessariamente sempre "appoggiati" ad un supporto di memorizzazione, per cui al momento del sequestro si può porre il problema di quale sia l'oggetto del provvedimento. Escludendo, se non in casi particolari, di estendere il sequestro a tutto l'apparato informatico e periferiche (come pure spesso è accaduto nel caso di sequestri di monitor, stampanti e quant'altro) l'asportazione materiale riguarderà normalmente solo le memorie di massa.

Spesso, in luogo del sequestro, l'Ufficio del Pubblico Ministero può orientare l'acquisizione degli elementi di prova attraverso lo strumento dell'ispezione, con un minore impatto sull'ordinaria attività del soggetto (specie quando il computer è utilizzato anche per motivi di lavoro, o trattasi di apparati informatici di aziende di grandi dimensioni), mediante l'effettuazione sul posto della copia "bitstream" delle memorie digitali da parte di un esperto di "computer forensics" in veste di ausiliario di P.G., compatibilmente con la situazione logistica e temporale contingente.

L'ispezione, attività tipica di polizia giudiziaria, (art. 244 e ss. c.p.p.) è caratterizzata dall'irripetibilità degli atti, con conseguente utilizzabilità degli atti compiuti in dibattimento. L'operatore deve, in contraddittorio con la parte esplorare ed analizzare i supporti informatici dell'indagato, alla ricerca di dati e tracce informatiche inerenti i fatti oggetto dell'ispezione, che saranno cristallizzati con i dovuti metodi in supporti durevoli, da allegare al relativi verbale.[11]

Il ricorso alla procedura dell'ispezione appare preferibile quando si procede per piccoli reati, in quanto, sovente si pongono dei problemi di ordine tecnico, atteso che, nel caso concreto, spesso non è possibile esaminare in loco una grande mole di dati, considerando anche quelli cancellati, che spesso appare particolarmente interessante, a fini investigativi, recuperare.

Questa opzione procedurale, pur presentando indubbi vantaggi, richiama i problemi tecnici di cui si è fatto cenno. Se eventuali modifiche del supporto originale in fase di copia possono essere evitate anche grazie a specifici strumenti hardware, più problematico, visto che il supporto rimane nella disponibilità dell'abituale utilizzatore, potrebbe essere garantire la perfetta identità tra originale e copia sia al momento dell'operazione che in tutte le fasi successive, fino all'eventuale dibattimento.

In particolare, per tutta la durata del procedimento bisognerà essere in grado di dimostrare che la copia sulla quale si eseguono gli accertamenti e che fornirà le

[11] **L'artt. 244 c.p.p**., novellato dalla legge 18 marzo 2008 n. 48, costituisce esempio di una rinnovata attenzione del legislatore alle tecniche di **computer forensic** per la ricerca delle evidenze digitali.. Quando le ispezioni riguardano tracce digitali, **l'autorità giudiziaria può disporre ogni operazione tecnica anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali ed impedirne l'alterazione**.

eventuali prove del reato sia perfettamente identica a quella in possesso dell'indagato (o del terzo non sottoposto ad indagini ma in possesso di materiale probatorio) al momento dell'intervento.

Anche quando si procede con sequestro, può essere opportuno lasciare il materiale in giudiziale custodia a chi lo detiene. Con ciò si ottiene il duplice risultato di:

- evitare il rischio di danneggiamento (e di richieste di risarcimento) degli apparati durante il trasporto e la custodia da parte della P.G. o presso gli uffici giudiziari;
- facilitare le operazioni dell'eventuale dissequestro.

Sia in caso di sequestro senza asportazione del materiale che in caso di ispezione, è importante **documentare l'assoluta identità tra dati originali e dati copiati.**

A tal fine, bisognerà acquisire sul posto **l'immagine bit stream**[12] di ogni memoria di massa, calcolando il **valore di hash**[13] sia dell'originale che dell'immagine (ovviamente i due valori *dovranno* coincidere); tutti i valori di hash calcolati dovranno essere stampati, formando parte integrante del verbale redatto dalla P.G. operante, nel quale risulterà anche l'indicazione del dispositivo hardware *write block* utilizzato per la copia.

In sostanza nella formazione dell'immagine dovrà essere creata una sorta di impronta, che contraddistinguerà in maniera univoca la traccia informatica oggetto di analisi, al fine di ottemperare alle esigenze di integrità del dato. Si procede ad operazione c.d. di hashing a senso unico con algoritmo classe MD5, che genera un' impronta dalla lunghezza di 128 bit (16 byte)

Con questa procedura difficilmente potranno essere mosse fondate contestazioni circa la genuinità, l'integrità e l'uguaglianza all'originale della copia acquisita. Tale copia

[12] La copia forense ha lo scopo di effettuare una duplicazione bit a bit del supporto oggetto di indagine. Mediante tale copia, deve essere possibile ricreare un supporto perfettamente identico, a livello logico, all'originale. Questo impone di copiare non solo i dati, ma qualunque informazione sia presente sul supporto, comprese le strutture di gestione, come master boot record, tabella delle partizioni, metadati del file system, spazio libero. Da tale considerazione si evince un principio importante, ovvero che la copia deve essere sempre della stessa grandezza (in termini logici) del supporto, indipendente dalla qualità e quantità di informazioni effettivamente contenute nel supporto stesso. Il metodo migliore per effettuare tale copia è considerare qualunque supporto come un supporto ad accesso sequenziale, simile ad un nastro magnetico. In tal modo sarà passibile leggere il disco bit a bit, partendo dal primo blocco sino all'ultimo.

[13] Al fine di garantire la non alterazione della prova, la copia ottenuta dovrà essere necessariamente validata; per far questo si utilizzano solitamente dei programmi di hash o message digest. Una funzione di hash è una funzione matematica non invertibile in grado di processare un dato arbitrariamente grande, e di calcolare da questo, un valore di grandezza fissa

potrà anche essere utilizzata per successivi accertamenti tecnici da parte di consulenti della difesa o periti nominati dal giudice.

La scelta di questa procedura andrà comunque valutata dagli organi inquirenti in relazione alle peculiarità dell'indagine, ma occorre sottolineare che anche nel caso di sequestro con asportazione del materiale, il metodo descritto garantisce la non ripudiabilità, da parte dell'indagato, dei dati acquisiti.

Il differimento della copia ad un'epoca successiva (normalmente all'esecuzione della consulenza tecnica per il P.M.) comporta invece la consegna dei supporti originali al C.T., il quale eseguirà la copia nel proprio laboratorio, da solo o comunque senza la presenza dell'indagato o del suo difensore. In questa procedura vi un intervallo di tempo, quello compreso tra la consegna del plico sigillato al C.T. ed il calcolo dell'hash sull'originale, che sfugge alla catena di custodia della prova digitale, prestando il fianco a possibili (anche se improbabili) contestazioni o dubbi sul valore probatorio della consulenza.

Una via di mezzo tra l'esigenza di una corretta acquisizione della prova e l'eventuale difficoltà nel compiere le operazioni di copia sul posto, ma attuabile solo in caso di sequestro con asportazione dei supporti, può consistere nell'eseguire in sede di intervento (alla presenza dell'indagato ed eventualmente di una persona di sua fiducia e del suo difensore) solo il calcolo dell'hash dei supporti da acquisire (operazione più veloce ma che soprattutto richiede pochissime risorse di memorizzazione rispetto alla copia contestuale), rimandando ad un secondo momento (in condizioni logistiche più favorevoli presso il laboratorio del C.T.) la copia e l'esame dei dati. In questo modo l'uguaglianza tra il valore di hash calcolato al momento del sequestro e quello calcolato sullo stesso supporto al momento della copia (verifica ripetibile in ogni momento successivo) fugherà ogni dubbio circa la correttezza della procedura e la genuinità della prova.

L'ufficio del Pubblico Ministero dovrà procedere quindi, con le forme dell'art. 360 c.p.p., solo nella fase di asportazione del supporto, formazione della "bit stream

immage" e calcolo del codice hash, mentre il consulente tecnico potrà , nel suo laboratorio, procedere, ai sensi dell'art. 359 c.p.p., all'esame del supporto clone, attraverso una procedura quindi che garantirà, in maniera certa e genuina la ripetibilità delle operazioni in dibattimento.

Al fine di poter inserire le attività informatiche svolte con il sistema in esame in un corretto panorama temporale è importantissimo **che chi opera l'acquisizione fisica e/o digitale documenti date e orario del sistema stesso**. Se consideriamo che i timestamp applicati dal sistema ai files, in seguito ad attività di creazione/modifica/accesso, sono legate a data/ora di sistema appare evidente che la mancata trasmissione di tali informazioni all'esaminatore potrà comportare una non corretta interpretazione degli eventi, ci si potrebbe così trovare, per esempio, nell'impossibilità di dimostrare che l'indagato , in uno specifico momento- rilevante a fini d'indagine- non stava utilizzando il sistema, con tutte le conseguenza del caso.

I principi di "computer forensic" trovano sempre più applicazione anche nelle fasi prodromi che e funzionali al sequestro, sovente e quasi necessariamente preceduto da attività di perquisizione.

La citata legge 18 marzo 2008 n. 48 ha novellato l'art. 247 c.p.p in tema di perquisizioni, introducendo un comma 1 bis in cui si prevede che "*Quando vi sia motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè 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*[14]"

Ipotesi particolare, rilevante ai fini della presente relazione, è quella prevista dal novellato art. 353 c.p.p., nella parte in cui concerne l'acquisizione di plichi , pacchi, valori, telegrammi o *altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica.* In tali ipotesi l'ufficiale di polizia giudiziaria , in via

[14] Trattasi di altra applicazione dei principi di computer forensic analoga a quella indicata nel novellato art. 244 c.p.p.

d'urgenza, possono ordinare al preposto al servizio postale, telegrafico, telematico o di telecomunicazione di **sospenderne l'inoltro.**

Importante appare la previsione del novellato art. 354 c.p.p., nella parte in cui, gli ufficiali di polizia giudiziaria, se vi è pericolo di dispersione o alterazione di cose o tracce pertinenti al reato, ancor prima dell'intervento del pubblico ministero, compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. *In relazione ai dati, alle informazioni ed ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali di p.g. adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione ed 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 ed alla sua immodificabilità.*[15]

La legge 48/2008 è intervenuta anche in tema di **sequestro di corrispondenza,** novellando l'art. 254 c.p.p. ed introducendo una nuova previsione normativa (art. 254 bis c.p.p.) prevedendo nella prima ipotesi il sequestro di corrispondenza anche se inoltrata per via telematica, che possano avere relazione con il reato.

Il nuovo art. 254 bis consente il sequestro presso fornitori di servizi informatici, telematici e di telecomunicazioni. I dati da sequestrare possono concernere anche **dati di traffico e di ubicazione e la loro acquisizione potrà avvenire anche mediante copia di essi su adeguato supporto, con 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.**

[15] Vd. Nota sub 10

Il sequestro preventivo.

La collocazione sistematica tra le misure cautelari fornisce una concreta dimensione del sequestro preventivo che, come tutte le misure cautelari, è caratterizzato **da una funzione specifica**, quella di evitare fatti tali da pregiudicare l'efficacia del provvedimento definitivo; in tal senso il sequestro è preordinato "alla emanazione di un ulteriore provvedimento definitivo, di cui previamente assicura la fruttuosità pratica"

È indubbio che proprio tale caratteristica induce ad attribuire al sequestro preventivo **il carattere della strumentalità** che lega inevitabilmente ogni provvedimento cautelare a quello definitivo; la fruttuosità del processo è attuata prevenendo il verificarsi di altri fatti criminosi.

Si tratta di una misura di coercizione reale, adottabile per esigenze di prevenzione, strumentale allo svolgimento del processo penale e all'accertamento del reato per cui si procede, nel senso che **è suo scopo quello di evitare che il trascorrere del tempo possa pregiudicare irrimediabilmente l'effettività della giurisdizione espressa con la sentenza di condanna.**

L'aggravamento del reato, la protrazione delle sue conseguenze e la commissione di altri reati costituiscono eventi tali da pregiudicare l'effettività del processo penale che è finalizzato anche a far diventare il reato "impossibile"; in tal senso, si afferma, *il sequestro preventivo opera come inibitoria di una condotta ritenuta pericolosa e riferita all'uso di una "cosa"*, sottoposta ad un vincolo di indisponibilità, idonea ad incidere su diritti costituzionalmente riconosciuti coma la libertà di manifestazione del pensiero, il diritto di proprietà, la libertà di iniziativa economica, la libertà di circolazione.

Per tali ragioni, è consolidata l'affermazione secondo cui il sequestro preventivo, pur raccordandosi nel suo presupposto giustificativo ad un fatto criminoso, può prescindere totalmente da qualsiasi profilo di colpevolezza, essendo ontologicamente legato non all'autore del reato, ma alla cosa che viene riguardata nell'ordinamento come strumento.

L'ordinamento tende a creare un quadro normativo dai contorni precisi, volto a limitare il rischio di abusi e ad ottenere un equilibrio fra difesa sociale e garantismo; a tal fine è stabilita **una riserva di giurisdizione e un principio di tassatività**, assegnando al solo giudice il potere di disporre la misura, così offrendo, attraverso la previsione codicistica dell'istituto, una base unitaria a figure contenute nelle leggi speciali, già presenti nell'ordinamento e che affioravano in modo frammentario nel codice abrogato.
Strettamente connessa alla esatta individuazione della funzione della misura coercitiva reale è anche la problematica dell'applicabilità al sequestro preventivo dei principi di proporzionalità, adeguatezza e gradualità, stabiliti per le misure cautelari personali dall'art. 275 c.p.p. La dottrina maggioritaria è per la tesi positiva, adducendo che la previsione di un potere di revoca parziale del sequestro, previsto dall'art. 324, comma 6, c.p.p., dovrebbe intendersi riferito pure alle ipotesi in cui la misura adottata sia "eccessiva" rispetto alle finalità cautelari perseguite; si assume, cioè, che l'ordinamento, pur non autorizzando il giudice ad una comparazione fra gravita del fatto e danno economico derivante dalla misura, gli imporrebbe comunque una disciplina finalizzata ad evitare la compressione ingiustificata dei diritti costituzionalmente garantiti, sui quali il sequestro viene ad incidere.

Il concetto di cose pertinenti al reato.

Il legislatore, contrariamente a quanto abbia fatto per il "*corpo del reato*", non ha individuato quali siano gli oggetti che costituiscono la categoria delle cose pertinenti al reato, affidando tale compito alla interpretazione giurisprudenziale .
Dottrina e giurisprudenza concordano nel ritenere che la nozione di cosa pertinente al reato abbia un significato ampio e comprensivo anche del corpo di reato, **cioè delle cose sulle quali o mediante le quali il reato è stato commesso,** e che il legame di pertinenza esprima un nesso causale fra *res* e reato, nella duplice prospettiva di una causalità consumata (illecito già commesso) e causalità potenziale (sviluppi criminali agevolati dalla libera disponibilità del bene).

E tuttavia, a fronte di un orientamento secondo cui tra la *res* e il reato deve intercorrere un rapporto di strumentalità, contraddistinto dal carattere della essenzialità e dalla stabilità, e non di mera occasionalità, **essendo necessario che la cosa rappresenti un mezzo indispensabile per l'attuazione e la prosecuzione dell'attività criminosa**, si registrano altre pronunce secondo cui, invece, non occorre che vi sia una relazione diretta e tipica tra le cose sequestrate e l'oggetto penale della fattispecie criminosa per la quale si indaga, **dovendosi includere nella nozione di cosa pertinente al reato, oltre al *corpus delicti*, tutte le cose che servono, anche indirettamente, ad accertare la consumazione del reato** con riferimento ad ogni possibile legame, caso per caso individuabile, tra le cose stesse e l'accertamento dell'illecito.
La giurisprudenza più recente sembra propendere per il primo degli orientamenti riferiti, ritenendo necessaria l'esistenza del rapporto strutturale e organico del bene con l'attività criminosa, sicchè esso deve trovarsi in una stretta correlazione con la commissione del reato, non essendo sufficiente che vi sia una sua qualsiasi utilizzazione strumentale alla commissione del fatto illecito.

I presupposti del sequestro preventivo L'art. 321 comma 1: il *fumus delicti* e lo standard probatorio richiesto.

L'art. 321 c.p.p., mentre individua espressamente quale debba essere il "*periculum*" necessario per disporre il provvedimento cautelare, non è altrettanto chiaro con riferimento al "*fumus*".
Il tema è strettamente legato al problema della **individuazione della soglia probatoria minima** richiesta per la sussistenza del vincolo della *res* al reato, di cui si è detto, nonché a quello della delimitazione della concreta sfera di incidenza delle finalità preventive della misura cautelare reale: il rischio di una lettura sbilanciata in senso estensivo o restrittivo della rilevanza assegnabile al requisito della pertinenzialità è quello di condurre ad un pericoloso soggettivismo nell'interpretazione di un enunciato normativo connotato, quantomeno, da una invincibile labilità prescrittiva.

In dottrina, a fronte di alcuni orientamenti tendenti ad evidenziare lo stretto parallelismo con le misure cautelari personali e a desumere, quindi, la necessità, per l'adozione del sequestro preventivo, dell'esistenza dei gravi indizi di colpevolezza, altra corrente di pensiero ritiene sufficiente la sussistenza di precisi indizi di reato e la coincidenza tra la fattispecie concreta e quella ipotizzata, ovvero, secondo ulteriori impostazioni, la necessità di un quadro indiziario grave in ordine alla avvenuta commissione del reato per cui si procede, alla pertinenza del bene da sottoporre a sequestro e alla libera disponibilità della cosa.

La giurisprudenza non ha mai dubitato della **necessità del *fumus*** ai fini della legittimità del provvedimento di sequestro preventivo e, tuttavia, quando ha dovuto stabilire in che cosa consiste il requisito in parola è giunta a conclusioni non univoche, in qualche modo strettamente conseguenziali alla particolare ampiezza della nozione di "cosa pertinente al reato" e alla difficoltà di qualificazione del tipo di relazione tra la *res* e il reato oggetto di accertamento.

Secondo il primo, prevalente, orientamento, presupposto del sequestro preventivo sarebbe la avvenuta commissione di un reato e a giustificare la misura coercitiva sarebbe sufficiente il *fumus* di sussistenza degli estremi del reato ipotizzato; sul piano probatorio, tale principio viene avvallato dall'affermazione secondo cui, quando l'indicazione del reato commesso non sia limitata ad un mero riferimento alla norma violata, ma sia, invece, supportata da elementi di fatto tali da renderla astrattamente ipotizzabile, non sarebbe necessaria né la individuazione dettagliata del fatto storico nei suoi limiti soggettivi o temporali, né i gravi indizi di colpevolezza, essendo precluso ogni sindacato sulla fondatezza della accusa e sulla prognosi di una pronuncia sfavorevole per l'imputato.

Secondo altra impostazione, invece, ai fini della emissione del provvedimento cautelare sarebbero non sufficienti gli indizi di commissione del fatto o del reato, ma sarebbe richiesta la probabile affermazione della responsabilità della persona sottoposa alle indagini.

Sul punto, sono intervenute in più occasioni le **Sezioni Unite della Corte di Cassazione** che hanno ribadito, in tema di condizioni generali di applicabilità, la distinzione tra misure cautelari personali e misure reali, attesa la diversa essenza valoristica dell'inviolabilità della libertà personale rispetto alla libera disponibilità dei beni: il fondamento giustificativo di una misura cautelare reale è costituito dal tasso di pericolosità in sé della cosa che, pertanto, pur raccordandosi ad un fatto criminoso, può prescindere totalmente da qualsiasi profilo di colpevolezza, essendo la misura cautelare reale non necessariamente legata all'autore del reato bensì, appunto, alla cosa.

Quanto allo standard probatorio richiesto ai fini della adozione della misura, la Corte di Cassazione ha in più occasioni chiarito che l'indagine del giudice di merito deve essere rivolta alla ricerca dei su indicati presupposti oggettivi, mentre l'elemento soggettivo del reato – che emerga in modo evidente sul piano fattuale- deve essere preso in considerazione solo in quei limitati casi in cui esso si riverbera sulla componente materiale, incidendo, cioè, sulla configurabilità stessa del reato.

Nondimeno incertezze permangono per ciò che concerne l'esatta definizione dei poteri di verifica spettanti al giudice chiamato ad applicare la misura: se è tendenzialmente ammessa l'applicazione di tale misura anche in assenza di una ben definita qualificazione giuridica del fatto e del suo autore, essa è senza dubbio esclusa quando un reato non sia stato ancora commesso.

È tuttavia con riferimento ai connessi poteri spettanti al tribunale del riesame, dinanzi al quale sia stato impugnato il provvedimento applicativo del sequestro probatorio, che sono stati meglio chiariti i contorni del presupposto in argomento; la verifica della legittimità del provvedimento applicativo non deve, secondo gli assunti nomofilattici, sconfinare nel sindacato della concreta fondatezza dell'accusa, ma deve limitarsi all'astratta possibilità di sussumere il fatto attribuito ad un soggetto in una determinata ipotesi di reato.

È consolidata l'affermazione secondo cui la verifica della sussistenza del *fumus commissi delicti* va compiuta sotto il profilo della congruità degli elementi rappresentati, che non possono essere censurati in punto di fatto per apprezzare la coincidenza con le reali

risultanze processuali, ma che vanno valutati, così come esposti, al fine di verificare se essi consentano di sussumere l'ipotesi formulata in quella tipica nonché l'esatta qualificazione dell'oggetto del provvedimento.

E tuttavia, al fine di limitare pericolosi soggettivismi, sempre più numerose sono le pronunce in cui si chiarisce che il controllo al quale è chiamato il giudice non può essere puramente formale, limitato, cioè, alla verifica dell'apparente legalità della misura cautelare adottata e ad una mera presa d'atto della tesi accusatoria, ma deve estendersi ad un esame della fattispecie concreta nei suoi estremi di tempo, di luogo, di indicazione della norma violata e delle ragioni per cui la fattispecie potrebbe integrare il reato ipotizzato.

(Segue): il periculm in mora.

Quanto sopra evidenziato impone di ritenere il *periculum in mora* non come generica ed astratta eventualità, ma come concreta ed attuale possibilità che il bene assuma carattere strumentale rispetto all'aggravamento o alla protrazione delle conseguenze del reato ipotizzato o alla agevolazione della commissione di altri reati; esso deve essere conseguenzialmente connesso al reato oggetto del procedimento penale e gli effetti che si intendono impedire sono quelli attinenti agli elementi strutturali dell'illecito, che con questi, cioè, siano collegati.

In tal senso si pone, si comprende e si giustifica il divieto di ammissibilità della misura cautelare in funzione di prevenzione *ante delictum:* il riferimento normativo alla commissione di "altri reati" non implica un giudizio di pericolosità legato alla probabilità astratta che alcuno commetta reati, ma circoscrive l'ambito di applicazione dell'istituto nei limiti segnati dall'attitudine della cosa ad essere, strumentalmente ma oggettivamente, collegata alla perpetrazione di altri fatti criminosi e dalla sua pertinenza all'illecito per cui si procede.

Le maggiori incertezze permangono in relazione alla configurabilità del *periculum in mora* nei reati che risultano già commessi e perfezionati in tutti i loro elementi costitutivi. L'indirizzo prevalente è nel senso di ritenere che il pericolo attinente alla libera disponibilità della cosa andrebbe inteso in senso oggettivo, come probabilità di danno futuro, connesso alla effettiva disponibilità materiale o giuridica della cosa o al suo uso, sicchè non sarebbe di ostacolo all'adozione della misura il fatto che il reato sia già consumato.

Il sequestro preventivo di sito web

La tematica del sequestro preventivo di un sito web offre notevoli spunti di riflessione sotto un duplice profilo, sia tecnico che giuridico.

Sorvolando sugli aspetti della questione più squisitamente tecnici, occorre evidenziare che lo strumento cautelare offre strade percorribili tutte le volte in cui attraverso un sito web siano commessi reati ed occorra prevenire la reiterazione dell'illecito.

Si pensi ad esempio all'ipotesi di diffamazione a mezzo internet, nel caso un cui sulle pagine di un sito web siano pubblicati contenuti lesivi dell'onore e della reputazione di una determinata persona, o ancora, le ipotesi di siti web che diffondano materiale pedopornografico, o che consentano il download di file musicali in violazione della normativa sul diritto d'autore.

Fondamentale, ai fini dell'applicabilità dell'istituto, appare non solo la valutazione del *fumus commissi delicti,* ma soprattutto quella della sussistenza del *periculum in mora*¸ in relazione al quale il disposto vincolo cautelare reale si presenta assolutamente necessario al fine che si possano aggravare o protrarre le conseguenze del reato in contestazione, evenienza che discenderebbe dalla libera disponibilità, in capo al gestore del sito e della pagina web oggetto del sequestro preventivo (cfr. Cass. Sez. V penale, 15 gennaio 2008 n. 17401)

Con riferimento alle problematiche legate al sequestro dei siti web, occorre sottolineare che il sequestro preventivo postula **un vincolo di effettiva apprensione della cosa** oggetto del provvedimento e non può sostanziarsi in un ordine imposto dall'Autorità giudiziaria a terzi volto ad inibire ogni collegamento con il sito web strumentale alla commissione del reato, non potendosi risolvere il sequestro preventivo in una "inibitoria atipica", stante il principio di necessaria tipicità delle misure cautelari previsto dal codice di procedura penale.

Il problema si è posto, con riferimento alla normativa sul diritto d'autore, nel caso di un sito internet che, attraverso un circuito peer-to-peer, agevolava lo scambio di file al di fuori degli ordinari e legali circuiti di commercializzazione dei beni oggetto di proprietà intellettuale.

Il sito in questione www.thepiratebay.org rendeva disponibili, sulle pagine web, codici alfanumerici in grado di identificare singoli file e di consentire agli utenti registrati di scambiare tra loro copie integrali o parziali dei file stessi. Il sito web si pone pertanto in rapporto di strumentalità rispetto alla commissione del reato.

Le indagini operate dalla polizia giudiziaria permettevano di acclarare che i server su cui era ospitato il sito erano allocati all'estero.

Il gip presso il Tribunale di Bergamo disponeva il sequestro preventivo del sito web disponendo che i fornitori di servizi internet (ISP) operanti sul territorio dello Stato inibissero l'accesso agli utenti italiani al sito indicato ed agli IP correlati. (Trib. Bergamo, sez. G.i.p. ord. Del 1.8.2008 n. 3277) .

Il Tribunale del riesame del capoluogo orobico, con ordinanza depositata in data 6.10.2008, pur riconoscendo la sussistenza nella fattispecie concreta di gravi indizi di reato a carico dei gestori del sito, annullava il provvedimento sulla scorta di considerazioni legate alla natura reale del sequestro preventivo, che non può imporre una condotta di facere (o non facere) a carico di soggetti estranei al reato (i fornitori di servizi internet) , "*non conoscendo il codice di rito un istituto atipico quale quello di cui all'art. 700 c.p.c.*".

L'acquisizione dei dati presso gli Internet Service Providers.

L'acquisizione dei dati presso gli Internet Service Providers si inquadra nel più ampio e complesso tema della "data retention" (o "data preservation") e in tale vasta cornice deve essere collocata ogni sua disamina scientifica, con un modello di analisi che integra le questioni tecniche proprie della materia informatica e telematica, con quelle più strettamente giuridiche.

L'acquisizione dei dati presso l'ISP, invero, può essere compiuta in maniera più corretta e consapevole se vi è la conoscenza di tutte le fasi di emivita dei dati stessi e delle procedure di loro acquisizione e osservazione, le quali, con un buon margine di approssimazione, possono essere riassunte in "**generazione", "conservazione", "acquisizione" e "analisi".**

La puntuale conoscenza di ciascuna delle suddette fasi porta, in primo luogo, alla presa d'atto dell'esistenza di un certo grado di rischio di alterazione dei dati nell'intera filiera e, conseguentemente, della necessità di adottare una serie di cautele ai fini di preservare la genuinità e la non ripudiabilità delle informazioni raccolte.

Il panorama italiano della "computer forensics", d'altronde, risente in qualche misura della mancanza di regole sufficientemente precise e di modelli di intervento condivisi, i quali si sono invece andati affermando da tempo, con particolare favore, nel mondo anglosassone. A motivo di tale mancanza e di una frequente genericità della legislazione interna, permane tuttora una certa disomogeneità di orientamenti in ambito forense e accademico.

Sebbene il tema dell'acquisizione dei dati presso l'ISP sia, dunque, assai vasto e controverso, la sua trattazione nel contesto di un incontro di studi incentrato sulle "*nuove frontiere della comunicazione e la criminalità*" con un focus specifico sulla "*diffusione telematica di materiale pedopornografico*", offre una prospettiva di analisi più nitida, delimita inoltre il perimetro della normativa di riferimento, e smorza infine il grado di

criticità e di contrapposizione che da tempo accompagnano il dibattito scientifico sulla "data retention" nell'intero scenario internazionale.

Com'è noto, la tormentata disciplina della conservazione dei dati informatici è sostanzialmente derivata da fonti comunitarie, e segnatamente dalle **direttive 2002/58/CE e 2006/24/CE,** nell'ambito di un contesto fortemente contrassegnato da un aspro dibattito – tutt'altro che risolto – teso a individuare il più corretto equilibrio tra esigenze di "data protection" e "data retention".

Le esigenze prevalenti di protezione dell'infanzia e di repressione dei delitti di sfruttamento sessuale dei fanciulli sembrerebbero, tuttavia, avere in qualche modo "stralciato" di fatto, tale materia dal contesto del dibattito principale, riconoscendo una tutela "rafforzata" al particolare bene giuridico da tutelare.

In questa logica si inquadra la **decisione del Consiglio dell'Unione Europea del 29 maggio 2000 (2000/375/GAI)** relativa alla lotta contro la pornografia infantile su internet, la quale dispone (art. 3 lett. c) che "*gli Stati membri esaminano le misure [..] per sollecitare i fornitori di servizi Internet [..] a conservare i dati relativi al traffico (delle telecomunicazioni) soprattutto ai fini delle azioni penali qualora si sospetti l'abuso sessuale di bambini, nonché la produzione, il trattamento e la diffusione di materiale di pornografia infantile*".

La decisione 375 non soltanto "*è obbligatoria in tutti i suoi elementi per i destinatari da essa designati*", ai sensi dell'art.249 del Trattato istitutivo della Comunità Europea, ma avendo essa a oggetto un *facere* specifico, risulta di conseguenza ben delimitata la discrezionalità di ogni singolo Paese entro il perimetro indicato dal testo della decisione stessa.

Per effetto dell'emanazione della decisione 2000/375/GAI, infatti, in materia di *data retention* con specifiche finalità di repressione dei delitti di sfruttamento sessuale dei bambini e di pedopornografia, è stato determinato l'*an,* ovvero la necessità di pervenire alla materiale conservazione dei dati relativi al traffico delle telecomunicazioni per quel fine precipuo, mentre è stato demandato all'apprezzamento discrezionale del singolo Stato membro sia il *quid* specifico sia il *quomodo* della conservazione.

Al fine di sgombrare il campo da eventuali dubbi di sorta, giova sottolineare che né la direttiva 2002/58/CE né la direttiva 2006/24/CE, hanno apportato modifiche o abrogazioni implicite o esplicite alla decisione 2000/375/GAI, i cui contenuti, al contrario, sono stati invece ribaditi e riaffermati dal Consiglio dell'Unione Europea con la decisione quadro **2004/68/GAI del 22 dicembre 2003** (pubblicata nella Gazzetta Ufficiale della Comunità Europea n. 13/44 L del 20 gennaio 2004) la quale afferma che: "*È necessario che la decisione 2000/375/GAI del Consiglio sia seguita da ulteriori iniziative legislative volte a dirimere le divergenze nelle impostazioni giuridiche degli Stati membri ed a contribuire allo sviluppo di una cooperazione efficace, a livello giudiziario e di applicazione delle leggi, nella lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile*".

Il suddetto richiamo alla decisione 375 offre peraltro lo spunto per sottolineare le sue differenti finalità rispetto a quelle della direttiva 2002/58/CE e di quella successiva n.2006/24/CE. Mentre queste ultime sono state emanate, infatti, in base all'art.95 del Trattato CE con lo scopo di armonizzare le legislazioni nazionali al fine di favorire il funzionamento del mercato interno, la decisione 2000/375/GAI è stata invece adottata con l'intento deliberato di "*prevenire e combattere lo sfruttamento sessuale dei bambini e, in particolare, la produzione, il trattamento, il possesso e la diffusione di materiale di pornografia infantile attraverso Internet*".

Alla luce delle precedenti considerazioni, appare evidente come il legislatore comunitario abbia disciplinato con strumenti giuridici differenti e con atti normativi separati la materia della conservazione dei dati con finalità di repressione dei delitti di pedopornografia da quella avente invece finalità di repressione della vasta categoria dei crimini informatici (o *computer crimes*).

Chiarito il differente percorso di individuazione della particolare e specifica fonte comunitaria circa l'obbligo di conservazione dei dati in materia di lotta alla pedopornografia, e le sostanziali differenze insite nelle finalità di tale fonte, per quanto invece concerne il *quid* e il *quomodo* della conservazione, l'analisi può essere ricondotta entro i binari delle regole generali, sostanzialmente definite nell'impianto normativo

interno dalla versione attuale dell'art.**132 del "codice della privacy"**, cui si aggiungono i provvedimenti del Garante per la protezione dei dati personali.

La generazione e conservazione dei dati del traffico telematico.

In tema di generazione e conservazione dei dati del traffico telematico rileva in primo luogo il profilo soggettivo, ovvero l'individuazione dei soggetti obbligati alla conservazione dei c.d. *file di log*.[16] La norma individua tali soggetti nei **"fornitori"** di comunicazione (sostanzialmente gli ISP), ma nelle ipotesi speciali di cui ai commi 4 *ter*, *quater* e *quinquies* dell'art.132 del "codice della privacy", recentemente introdotti dalla legge 48/2008 (compresa l'ipotesi di cui all'art.600-ter comma 1 CP), ai "fornitori" devono ora aggiungersi **gli "*operatori*"** di servizi informatici e telematici, rispetto ai quali, in assenza di una definizione del termine "operatore" e dovendosi distinguere quest'ultimo dal "fornitore", sembra di capire che ci si riferisca in maniera indiscriminata ai fornitori di contenuti e di servizi (per esempio, ai motori di ricerca, ma anche ai contatori, ai broker pubblicitari nel web, e addirittura a tutti i "content provider").

Rileva inoltre il profilo oggettivo, ovvero l'indicazione d**i quali dati generare** e conservare, dovendosi considerare assai generica la definizione contenuta nella norma di "**dati relativi al traffico**". L'unico parametro di riferimento per l'individuazione analitica dei "dati" da generare e conservare è al momento definito, con procedimento *ex adverso*, dai provvedimenti del Garante che ribadiscono il divieto della conservazione di taluni dati (per esempio, il contenuto delle comunicazioni) e che impongono (ancora una volta in modo assai generico) i principi di "pertinenza" e di "non eccedenza", ma

[16] I **File di log** sono file in cui si tengono registrate le attività compiute per esempio da un'applicazione, da un server, o da un interprete di comandi. Ad ogni collegamento sul server relativo al sito web visitato, vengono scritte informazioni relative all'accesso dell'utente (IP address, data, ora, pagina richiesta, login, account). Profili di analogia, sotto il profilo della "data retention" presentano i **cookies,** che sono brevi stringhe alfanumeriche che il server invia al browser dell'utente quando questi si connette per la prima volta, allo scopo di immagazzinare specifici dati. Successivamente il browser dell'utente invia una copia del cookie al server in occasione di ogni nuova connessione in modo da permettere al provider di ricordare i dati del visitatore.

tutto ciò non vale a colmare le carenze derivanti dalla mancanza di una definizione di "dati relativi al traffico".

La direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 *riguardante la conservazione di 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*, enumera le "categorie di dati da conservare" (art.5), i quali, con riferimento a internet, sono:

a) **i dati necessari per rintracciare e identificare la fonte di una comunicazione per l'accesso Internet, posta elettronica su Internet e telefonia via Internet**:

i) identificativo/i dell'utente;

ii) identificativo dell'utente e numero telefonico assegnati a ogni comunicazione sulla rete telefonica pubblica;

iii) nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico

b) **i dati necessari per rintracciare e identificare la destinazione di una comunicazione (limitatamente alla telefonia fissa e mobile e alla posta elettronica con esclusione implicita dei dati relativi all'accesso a internet)**

c) **i dati necessari per determinare la data, l'ora e la durata di una comunicazione**:

i) data e ora del log-in e del log-off del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo IP, dinamico o statico, assegnato dal fornitore di accesso Internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato

d) i dati necessari per determinare il tipo di comunicazione (limitatamente alla telefonia fissa e mobile e alla posta elettronica con esclusione implicita dei dati relativi all'accesso a internet)

e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature:

- per l'accesso Internet, la posta elettronica su Internet e la telefonia via Internet:

  i) numero telefonico chiamante per l'accesso commutato (dial-up access);

  ii) digital subscriber line (DSL) o un altro identificatore finale di chi è all'origine della comunicazione

f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile:

1) etichetta di ubicazione (Cell ID) all'inizio della comunicazione;

2) dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni.

Il comma 2 dell'articolo 5 recita infine: "***A norma della presente direttiva, non può essere conservato alcun dato relativo al contenuto della comunicazione***".

Il punto sub b) appare assai rilevante ai fini della possibilità concreta di poter conseguire gli scopi della norma, ovvero la repressione dei reati. Tale punto non annovera, infatti, la possibilità di conservare i dati necessari per rintracciare e identificare la destinazione di una comunicazione con riguardo all'accesso a internet, ma limita tale conservazione alla telefonia e alla posta elettronica. Esclusione, questa, che è in grado di vanificare le finalità della norma se ciascun utente della rete non viene

contraddistinto di tempo in tempo con un IP univoco, circostanza che non è tecnicamente possibile garantire nelle ipotesi di "IP masquerading" .

È il caso, assai frequente in Italia, delle reti NAT che presentano una moltitudine di utenti vero l'esterno con un solo IP pubblico.

La prassi di non conservare i dai relativi all'IP di destinazione della comunicazione telematica, unita all'assegnazione del medesimo IP pubblico a una moltitudine di utenti, rende tecnicamente vano ogni tentativo di identificazione degli autori di eventuali reati.

Al momento (aprile 2009) è consentito agli ISP operanti in Italia di fare ricorso alle reti "nattate", ma il Dlgs 30 maggio 2008 n. 109 ha introdotto l'obbligo per i "fornitori" di "*assicurare la disponibilità e l'effettiva* ***univocità*** *degli indirizzi di protocollo internet*". Tale obbligo non è ancora entrato in vigore, essendo stati prorogati i termini di adempimento con decreto legge, poi modificato in sede di conversione.

Rileva infine, sempre sul piano oggettivo, l'adozione di tutti gli accorgimenti tecnici utili a garantire una corretta generazione e conservazione dei dati, ma anche l'esigenza di pervenire a una normalizzazione dei diversi formati di generazione dei dati.

L'acquisizione dei dati del traffico telematico.

L'art.132 del codice della privacy impone la conservazione dei dati ***"per finalità di accertamento e repressione dei reati"***, motivo per cui il Garante per la protezione dei dati personali ha invitato i fornitori a non corrispondere a richieste di acquisizioni aventi finalità diverse (ALLEGATO A, n.5 lett.a, del Recepimento normativo in tema di dati di traffico telefonico e telematico - 24 luglio 2008, in G.U. n. 189 del 13 agosto 2008).

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.

Giova sottolineare che valgono per i log tutte le considerazioni che vengono svolte in materia di acquisizione probatoria del dato digitale rispetto all'esigenza di ridurre al minimo il rischio di alterazione. Sempre più spesso, d'altronde, alle lacune derivanti dall'esistenza di norme assai generiche si sommano alcune carenze di specializzazione nel mondo forense.

La questione relativa all'acquisizione dei log presso l'ISP è priva di riscontri giurisprudenziali significativi[17]. La prassi consolidata è quella di acquisire i dati formulando una richiesta direttamente al fornitore, delegando quest'ultimo a effettuare l'estrazione, la duplicazione e la trasmissione dei dati all'autorità richiedente.

È ancora aperto il dibattito circa la natura di tale atto di acquisizione, e in particolare se esso costituisca un "accertamento tecnico" in senso stretto, e inoltre se lo stesso, in quanto tale, sia ripetibile.

Si tratta evidentemente di questioni di particolare rilevanza (si pensi per esempio all'ipotesi dell'incidente probatorio), le quali possono essere sviscerate se, come si diceva in premessa, si è in grado di conoscere nel dettaglio le modalità tecniche di generazione e conservazione dei dati del traffico.

La già citata esigenza di poter contare su modelli e linee guida condivisi nella computer forensics, qui emerge in tutta la sua evidenza, laddove si potrebbe auspicare l'adozione di vere e proprie regole tecniche di generazione e conservazione dei dati, utili a garantirne l'immodificabilità.

Si pensi, per esempio, a un delitto informatico commesso nei confronti di un ISP da parte di un suo stesso cliente/abbonato. In quel caso, l'acquisizione dei log, nelle modalità consolidatesi nella prassi, sarebbe rivolta direttamente alla parte offesa, in totale assenza di garanzie circa l'integrità dei dati.

Nel caso di alcuni particolari delitti, peraltro, i file di log rappresentano l'unico elemento probatorio esistente, mentre nell'ambito delle indagini per la repressione dei delitti di pedopornografia, soccorrono gli accertamenti tecnici successivi

[17] Si segnala sul punto una pronuncia del Tribunale di Chieti (Sent. N. 175/2006) in cui l'imputato viene assolto ai sensi dell'art. 530 comma II° c.p.p. in quanto il procedimento di acquisizione dei file di log non è stato ritenuto proceduralmenet corretto e comunque non in grado di garantire la genuina acquisizione del dato – semplice richiesta al provider da parte della polizia giudiziaria-

all'acquisizione dei file di log, i quali offrono un riscontro oggettivo ai dati del traffico telematico. Si pensi, per esempio, al riscontro del ritrovamento della copia locale di un sito internet a contenuto pedopornografico nel computer sequestrato al soggetto indagato per il reato previsto dall'art.600-ter CP.

Deve osservarsi che in ambito forense, in realtà, è presente in qualche caso la tendenza a non conferire piena autonomia probatoria ai file di log, forse proprio in ragione dell'assenza di alcune fondamentali garanzie nel processo sotteso alla loro acquisizione.

Si pensi all'esempio da ultimo citato, nel quale i file di log indichino in maniera univoca un soggetto quale creatore e gestore di un sito internet a contenuto pedopornografico, ma tutti gli accertamenti esperiti sui computer sequestrati a quel soggetto risultino essere negativi. In questo caso, i file di log costituirebbero l'unico elemento probatorio disponibile e l'intera partita si giocherebbe sull'analisi dell'attendibilità dei dati acquisiti.

L'acquisizione di un file di log ha obiettivamente le caratteristiche di un accertamento tecnico non ripetibile, giacché l'elemento è per sua natura soggetto a continua mutazione (viene aggiornato in continuazione dal sistema) ed impone quindi il ricorso ai criteri di cui all'art 360 c.p.p..

E infatti è appena il caso di evidenziare che, se vi sono regole che stabiliscono i tempi di conservazione di alcuni tipi di dati, nessuna norma detta regole tecniche per detta conservazione, che garantiscano l'immodificabilità dei dati ad opera dell'amministratore di sistema e la possibilità di ricostruire l'attività svolta su tali elementi.

L'analisi dei log in ambito forense deve essere svolta da operatori qualificati e, stante la mole notevole di dati da esaminare, deve realizzarsi con l'impiego di strumenti software specifici. Generalmente, tale analisi è ripetibile, stante la relativa facilità a mantenere integro il dato probatorio.

L'esame dei log deve essere scrupolosamente documentato in tutti i suoi procedimenti, deve essere indicato l'impiego di hardware, sistemi operativi, tools specifici, con eventuali licenze d'uso.

L'analisi dei log terrà conto della configurazione dell'orario nel sistema che li ha generati.

****

La legge 48/2008 è intervenuta a modificare anche il codice in materia di protezione dei dati personali introducendo un nuovo comma all'articolo 132[18] Decreto legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali).

[18] Art. 132 (1)
Conservazione di dati di traffico per altre finalità

1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico [,inclusi quelli concernenti le chiamate senza risposta], sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, 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, sono conservati dal fornitore per dodici mesi dalla data della comunicazione. (2)

1-bis. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni. (3)

[2. Decorso il termine di cui al comma 1, i dati relativi al traffico telefonico sono conservati dal fornitore per ulteriori ventiquattro mesi per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.] (4)

3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del giudice su istanza del pubblico ministero o 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. (5)

[4. Dopo la scadenza del termine indicato al comma 1, il giudice autorizza l'acquisizione dei dati, con decreto motivato, se ritiene che sussistano sufficienti indizi dei delitti di cui all'articolo 407, comma 2, lettera a), del codice di procedura penale, nonchè dei delitti in danno di sistemi informatici o telematici.] (4)

[4-bis. Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati relativi al traffico telefonico con decreto motivato che è comunicato immediatamente, e comunque non oltre ventiquattro ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non è convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati.] (4)

4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative traniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i

Si tratta del comma 4-ter : «Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, **ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i**

---

dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi. (6)

4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca piu' grave reato, le disposizioni dell'articolo 326 del codice penale. (6)

4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia. (6)

5. Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'art.17, volti anche a:

a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato b);
b) disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1;
c) individuare le modalità di trattamento dei dati da parte di specifici incaricati del trattamento in modo tale che, decorso il termine di cui al comma 1, l'utilizzazione dei dati sia consentita solo nei casi di cui al comma 4 e all'articolo 7;
d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui ai commi 1 e 2.

[6. Le modalità di trattamento dei dati di cui al comma 5 sono individuate con decreto del Ministro della giustizia, di concerto con il Ministro dell'interno, con il Ministro delle comunicazioni e con il Ministro per l'innovazione e le tecnologie, su conforme parere del Garante]

(1) Articolo così sostituito dal D.L. 24 dicembre 2003, n. 354.
(2) Comma così da ultimo modificato dal Decreto legislativo 30 maggio 2008, n. 109.
(3) Comma inserito dal Decreto legislativo 30 maggio 2008, n. 109.
(4) Comma abrogato dal Decreto legislativo 30 maggio 2008, n. 109.
(5) Comma così modificato dal D.L. 27 luglio 2005, n. 144.
(6) Comma inserito dal Decreto Legge 23 maggio 2008, n. 92.

contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, **ovvero per finalità di accertamento e repressione di specifici reati.** Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

Comma 4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale.

4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia».