

Antonio Vele

**LA NATURA DELLE
COMUNICAZIONI CONTENUTE
NELLA MEMORIA DEL TELEFONO
CELLULARE NELL'AMBITO DEL
PROCEDIMENTO PENALE**

Estratto



Milano • Giuffrè Editore

GIURISPRUDENZA

CASSAZIONE

SEZ. V PENALE

16 GENNAIO 2018

N. 1822

PRESIDENTE: LAPALORCIA

ESTENSORE: MOROSINI

RICORRENTE: PARODI

Comunicazioni elettroniche

• Messaggi SMS e WhatsApp
 • Sequestro penale • Natura di documenti • Applicabilità dell'art. 243 c.p.p. • Disciplina sulla corrispondenza • Inapplicabilità.

I dati informatici acquisiti dalla memoria di un telefono in uso alla persona indagata (sms, messaggi WhatsApp, messaggi di posta elettronica “scaricati” e/o conservati

nella memoria dell'apparecchio cellulare) hanno natura di documenti ai sensi dell'art. 234 c.p.p. La relativa attività acquisitiva non soggiace né alla disciplina dettata dall'art. 254 c.p.p. per la corrispondenza, in quanto i testi SMS e WhatsApp non rientrano nel concetto di “corrispondenza”, la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito, né alla disciplina delle intercettazioni telefoniche.

**LA NATURA DELLE
 COMUNICAZIONI
 CONTENUTE NELLA
 MEMORIA DEL TELEFONO
 CELLULARE NELL'AMBITO
 DEL PROCEDIMENTO
 PENALE**

1. La natura delle comunicazioni contenute nella memoria del telefono cellulare nell'ambito del procedimento penale.

La recente sentenza del giudice di legittimità offre lo spunto per una riflessione sulla natura del documento informatico ed in particolare sugli aspetti problematici in ordine all'acquisizione dello stesso ad opera dei soggetti di polizia giudiziaria.

La Corte di cassazione, con la pronuncia in commento, evidenzia

che i dati informatici acquisiti dalla memoria del telefono in uso all'indagata (sms, messaggi *whatsApp*, messaggi di posta elettronica “scaricati” e/o conservati nella memoria dell'apparecchio cellulare e sottoposti a sequestro) hanno natura di documenti ai sensi dell'art. 234 c.p.p., evidenziando che la relativa attività acquisitiva non va confusa con le regole previste per la corrispondenza *ex art.* 254 c.p.p., in quanto la nozione di “corrispondenza” implica un'attività di spedizione in corso o

* La sentenza è riportata per esteso in questa *Rivista* 2018, 95.

comunque avviata dal mittente mediante consegna a terzi per il recapito; ancora, secondo la Corte, non è configurabile neppure un'attività di intercettazione, che postula, per sua natura, la captazione di un flusso di comunicazioni in corso. Nel caso di specie, infatti, ci si è limitati ad acquisire *ex post* il dato, conservato in memoria.

Nella stessa sentenza la Corte, infine, si afferma che alcuna violazione di legge sussiste per mancato rispetto del principio di proporzionalità e adeguatezza, essendosi proceduto, tramite duplicazione di copia forense, alla integrale e indiscriminata apprensione di tutti i dati archiviati nella memoria del telefono cellulare in uso all'indagata; e ciò perché l'acquisizione di dati informatici mediante la cd. copia forense è una modalità conforme a legge, che mira a proteggere, nell'interesse di tutte le parti, l'integrità e affidabilità del dato così acquisito. Di conseguenza il giudice di legittimità osserva come il sequestro di supporti contenenti dati informatici rilevanti e non pertinenti al reato poi restituiti, previa estrazione di copia integrale della relativa memoria, è un'attività legittima, a maggior ragione che per la selezione degli stessi occorre una complessa attività di analisi, che non può svolgersi nel limitato tempo del sequestro.

2. Ambito di applicazione processuale: sequestro o intercettazione dei dati comunicativi contenuti nella memoria di uno strumento elettronico?

L'interpretazione contenuta nella pronuncia annotata risulta condivisibile, in quanto i dati informatici rientrano nella categoria della prova documentale ai sensi dell'art. 234 c.p.p., essendo precostituiti e quindi già formati senza l'apporto dei soggetti del procedimento penale ¹.

Con tale formulazione normativa il legislatore ha ritenuto di non poter confinare tutti i mezzi già conosciuti e quelli non prevedibili per l'evolversi della scienza, al fine di ricomprendere nella citata previsione ulteriori forme di documenti offerte dal progresso tecnologico: l'art. 234 c.p.p. comma 1 c.p.p., infatti, contiene un'apertura, laddove consente l'acquisizione di qualsiasi altro mezzo, oltre ai documenti scritti e a quelli che rappresentano fatti, persone o cose attraverso la fotografia, la cinematografia e la fonografia.

Il documento informatico è un documento non cartaceo formato dai programmi (*software*) di un calcolatore elettronico e, contemporaneamente alla sua formazione, registrati in un apposito spazio del calcolatore medesimo (*hardware*) o su strumenti di supporto elettronico o digitale, quali *pen-drives*, *dvd*, *cd-rom*, etc. ²; possiamo, pertanto, definire il documento informatico come qualsiasi *file* avente un elemento rappresentativo espresso in linguaggio binario: un testo, un'immagine, un suono, quindi, anche una pagina *web* o una *e-mail* ³.

¹ Corte cost., 27 aprile 1995, n. 136, in *Giur. cost.*, 1995, 1062, secondo cui la natura di documento *ex art.* 234 c.p.p. si determina dal fatto che il medesimo ha origine nel processo penale e non è finalizzato ad esso.

² In riferimento a tale nozione di documento informatico cfr. L. P. COMOGLIO, *Le prove civili*, Torino, 2010, 529.

³ Su questa definizione v. G. VACIAGO, *Profili processuali delle indagini informatiche*, in *Diritto dell'internet*, a cura di G. Cassano-G. Scorza-G. Vaciago, Padova, 2013, 640. In informatica e nella teoria dell'informazione, il *bit* (inteso come "cifra binaria", dall'inglese "*binary digit*") può essere definito come unità elementare del-

In quest'ambito ontologico, la concezione tradizionale del documento resta ancora valida ⁴: il documento è uno strumento che fa conoscere un fatto e questa definizione può essere estesa anche al documento informatico.

Con il documento, di fatto, l'effetto conoscitivo viene realizzato attraverso la tecnica della rappresentazione, ossia il soggetto non ha diretta percezione di un determinato fatto, ma si rappresenta (e conosce) quello stesso fatto attraverso le "sensazioni" che gli provengono dalla percezione del documento; tale ricostruzione concettuale è applicabile anche al documento informatico, sebbene quest'ultimo risulti "dematerializzato" ⁵, nel senso che sussiste a prescindere « dal supporto fisico sul quale è incorporato » ⁶. Vi è quindi una necessaria base materiale che contiene la rappresentazione informatica di dati e fatti ⁷.

l'informazione trattata da un elaboratore. In questo contesto, il *bit* è dunque uno dei due simboli del sistema numerico binario, classicamente chiamati zero (0) e uno (1): il bit rappresenta quindi, in realtà, l'unità di definizione di uno stato logico, la cui rappresentazione è costituita dai soli valori 0 e 1. Ai fini della programmazione, è comune raggruppare sequenze di bit in entità più vaste che possano assumere valori in intervalli più ampi di quello consentito da un singolo bit; questi raggruppamenti contengono generalmente un numero di stringhe binarie pari a una potenza binaria, pari cioè a 2^n ; il più comune tra questi raggruppamenti è il *byte* (o "ottetto"), corrispondente a 8 *bit*, che costituisce l'unità di misura più utilizzata in campo informatico. Storicamente, un *byte* era il numero di bit utilizzati per codificare un "singolo carattere di testo" in un computer; il *byte* è anche la quantità minima d'informazione normalmente indirizzabile da parte di un microprocessore e utilizzabile nella programmazione ed è perciò divenuto l'elemento base come unità di misura delle capacità di memoria. Il *byte*, in quanto tipicamente formato da 8 *bit*, è in grado di assumere $2^8 = 256$ possibili valori (da 0 a 255), cui corrispondono altrettante diverse possibili combinazioni di una sequenza di 8 bit (ovvero di 8 "0" e/o "1"), in tema cfr., voce *informatica* (voce *byte-bit* e voci correlate). In prospettiva generale cfr. R. BORRUSO, voce « *Informatica giuridica* », in *Enc. dir.*, Agg., I, Milano, 1997, abcd.

⁴ Resta attuale la concezione tradizionale, in quanto il documento è una cosa che ha in sé la virtù del far conoscere e quest'ultima è dovuta a ciò che si definisce il contenuto rappresentativo, sul punto, v. F. CARNELUTTI, *Documento*, in *Nss. d. it.*, VI, Torino, 1960, 86; più di recente in tema di prova documentale cfr. L. KALB, *Il documento nel sistema probatorio*, Torino, 2000, 95; A. LARONGA, *La prova documentale nel processo penale*, Torino, 2004, 10 ss.; volendo, A. VELE, Art. 234 c.p.p., in *Commento codice di procedura penale*, a cura di Tranchina, Milano, 2008, I, 1765 ss..

⁵ L'aggettivo "dematerializzato" fa comprendere bene la caratteristica del documento informatico, vale a dire che il contenuto del documento informatico è autonomo dal supporto sul quale viene di volta in volta trasferito, in tal senso F. F. ALCARO, *Riflessioni, vecchie e nuove in tema di beni immateriali. Il diritto d'autore nell'era digitale*, in *Rass. Dir. civ.*, 2006, 951.

⁶ In tal senso, P. TONINI, *Manuale di procedura penale*, Milano, 2017, 365-366; l'autore, alla luce del progresso tecnologico, osserva che « oggi i metodi di incorporamento sono due: quello analogico e quello digitale. a) attraverso il *metodo analogico* la rappresentazione è incorporata su di una base materiale mediante grandezze fisiche variabili con continuità. L'incorporamento è "materiale" nel senso che la rappresentazione non esiste senza quel supporto fisico sul quale è stata incorporata. L'incorporamento è "materiale" nel senso che la rappresentazione non esiste senza quel supporto fisico sul quale è stata incorporata. Lo strumento che opera l'incorporamento può essere manuale (es. scrittura o disegno) o automatico (es. fotografia, fonografia o cinematografica); b) attraverso il *metodo digitale* la rappresentazione è incorporata su di una base materiale mediante grandezze fisiche variabili con discontinuità: si tratta di numeri, zero e uno. Il dato che contiene l'informazione è denominato informatico ed è composto dalla sequenza di *bit*. Il documento informatico ha la caratteristica di essere dematerializzato, nel senso che il documento esiste indifferentemente dal supporto fisico sul quale è incorporato, anche per la sua esistenza, richiede comunque l'incorporamento su di una base materiale: *hard disk*, *pen drive*, *CD* o altro strumento idoneo. La caratteristica del documento informatico, ed il suo pregio, è quella di essere trasferibile con rapidità da un supporto ad un altro, rimanendo identico ».

⁷ V. nota 6; in argomento cfr. P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. e proc.*, 2009, 401 e ss.

Per quanto riguarda l'attività di acquisizione dei documenti informatici, la pronuncia oggetto di riflessione evidenzia la sostanziale diversità tra la disciplina del sequestro di corrispondenza e quella del sequestro ordinario, oltre a far emergere che il flusso di comunicazioni non in atto esula dalla disciplina delle intercettazioni.

Sul punto, le Sezioni unite hanno delineato il concetto giuridico di corrispondenza, osservando, infatti, che la materia delle intrusioni investigative sulla "corrispondenza" è regolata dall'art. 254 c.p.p., che, rispetto alla normativa generale in tema di sequestri (art. 253 c.p.p.), si atteggia quale disciplina speciale, in quanto incidente su aspetti presidiati dall'art. 15 Cost. (nonché dall'art. 8 della CEDU), e che ha ad oggetto il sequestro della corrispondenza presso gestori (anche privati) di servizi postali; mentre hanno specificato che nessuna speciale ragione di tutela — salve le peculiari esigenze attinenti ai rapporti tra imputato e difensore (art. 103 c.p.p. e art. 35 disp. att. c.p.p.) e le limitazioni imposte alla polizia giudiziaria nell'acquisizione di "pliche sigillati o altrimenti chiusi", distinti dalla "corrispondenza" (art. 353 comma 1 c.p.p.) — interferisce con l'adozione di un ordinario provvedimento di sequestro da eseguire in qualsiasi luogo ove si trovino lettere o pieghi non ancora avviati dal mittente al destinatario o già da quest'ultimo ricevuti, in quanto simili cose non sono appunto "corrispondenza", implicando tale nozione un'attività di spedizione in corso o alla quale il mittente abbia dato comunque impulso consegnandola ad altri per il recapito⁸.

Per quanto concerne, dunque, il profilo dei dati comunicativi presenti nella posta elettronica, dalle *chat line* private ai messaggi, occorre tracciare un distinguo tra la corrispondenza ordinaria in corso di spedizione e quella contenuta nella memoria di un *computer*; questa differenziazione è importante per separare l'area operativa del sequestro ordinario rispetto all'area operativa del sequestro di corrispondenza: le comunicazioni contenute nella memoria di un *computer* oppure in un programma di gestione di posta elettronica (non ancora spedite o giunte al destinatario), dovrebbero rientrare nel cono d'ombra del sequestro ordinario (art. 253 c.p.p.). A questo proposito è bene precisare che il segreto epistolare rimane fin quando la missiva mantiene il valore di comunicazione attuale (una volta spedita), poiché protetta dall'art. 15 Cost.; in altri termini troverebbero applicazione le regole previste per l'attività di apprensione della corrispondenza (artt. 254 e 353 c.p.p.) anche al messaggio digitale che non ancora è stato letto (scaricato) dal destinatario⁹, ancorché risulta più complicato differenziare, da parte dei soggetti di polizia giudiziaria, il dato storico dalla comunicazione in corso di spedizione contenuti nella

⁸ Così, Cass. pen., Sez. Un., 19 aprile 2012, Pasqua, in *CED*, 252893; Cass. pen., sez. VI, 13 ottobre 2009, *ivi*, 245183.

⁹ In questa prospettiva cfr. ZACCHÉ, *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. e giust.*, 2013, 110, secondo cui in relazione alla posta elettronica già letta e archiviata dal destinatario nell'apposita cartella non si applicano le regole sulla corrispondenza, in quanto la comunicazione non è più attuale; viceversa risulta coperta dall'art. 15 Cost.;

ancora, l'autore evidenzia una possibile illegittimità costituzionale dell'art. 354 comma 2 c.p.p., giacché in assenza di un'autorizzazione preventiva dell'autorità giudiziaria, non dovrebbe essere consentito alla polizia giudiziaria di procedere all'apprensione con il sequestro della corrispondenza elettronica, oltre a non accedere alla relativa casella. In argomento v. L. LUPÁRIA, *La disciplina processuale e le garanzie difensive*, in Lupária-Ziccardi, *Investigazione penale e tecnologia informatica*, Milano, 2007, 172.

memoria di uno strumento tecnologico, nel rispetto della segretezza epistolare.

In questa chiave di ragionamento è utile specificare come il sequestro di corrispondenza, pur ricevendo protezione dall'art. 15 Cost., non rientra nella disciplina delle intercettazioni in senso stretto, a causa del diverso oggetto, implicando così una differenza sul piano strutturale.

La corrispondenza, infatti, essendo costituita da un documento o altra *res* contenente una comunicazione, può essere oggetto di apprensione coattiva, laddove sussistano i presupposti per l'applicazione della disciplina del sequestro, esulando dall'intercettazione, in quanto trattasi di una comunicazione precostituita (diversamente dallo strumento intercettativo che fonda su una interferenza o intromissione attraverso determinati dispositivi offerti dalla tecnica, rivolto ad apprendere in tempo reale le comunicazioni altrui). In sostanza, la diversità di oggetto comporta un differente potere dell'autorità, nonché presupposti e modalità esecutive nella compressione dei diritti fondamentali delle persona (il sequestro è un atto a sorpresa ma palese, invece l'intercettazione è un atto a sorpresa ma opera "dietro le quinte"); il limitato collegamento tra le due attività o l'affinità tra esse è riconducibile all'identità del diritto costituzionale sul quale le stesse incidono. In pratica, con il sequestro di corrispondenza si viola la segretezza della comunicazione, bloccando altresì l'*iter* della corrispondenza; nell'intercettazione, invece, non si realizza alcun impedimento o interruzione della comunicazione, ma un'apprensione insidiosa del dialogo tra i comunicanti.

In linea con la suddetta argomentazione le Sezioni unite hanno enunciato il seguente principio di diritto: la disciplina delle intercettazioni di conversazioni o comunicazioni, di cui all'art. 266 c.p.p. e ss., non è applicabile alla corrispondenza, dovendosi per la sottoposizione a controllo e la utilizzazione probatoria del contenuto epistolare seguire le forme del sequestro di corrispondenza di cui agli artt. 254 e 353 c.p.p.¹⁰.

In quest'ottica la Corte costituzionale, tenendo in considerazione la rappresentata interpretazione del giudice di legittimità, osserva che, seppur garantita la corrispondenza dall'art. 15 Cost., la tutela del diritto di comunicazione non esige l'uniformità della disciplina delle misure restrittive ad esso applicabile¹¹. Di qui la distinzione tra regole per l'attività di intercettazione e quelle per il sequestro della corrispondenza a garanzia dei diritti fondamentali.

Problematica poi è la questione del sequestro di informazioni scambiate tra indagato e difensore, in quanto la Corte di cassazione, nella sentenza annotata, afferma la non applicazione delle regole del sequestro di corrispondenza, qualora i messaggi digitali non siano in corso di spedizione, essendo inconferente il richiamo al divieto di cui all'art. 103, comma 6, c.p.p. In quest'ambito, però, rileva la riservatezza del messaggio comunicativo tra indagato-imputato e difensore e la finalità difensiva del medesimo.

¹⁰ Cass., Sez. Un., 18 luglio 2012, Pa-squa, cit.

¹¹ Corte cost., 24 gennaio 2017, n. 20, in www.cortecostituzionale.it.

Tale interpretazione, tuttavia, potrebbe collidere con il suindicato divieto di « sequestro e ogni forma di controllo della corrispondenza tra l'imputato e il proprio difensore..., salvo che l'autorità giudiziaria abbia fondato motivo di ritenere che si tratti di corpo del reato (art. 103 comma 6 c.p.p.) », qualora tale impedimento si estenda anche su comunicazioni digitali (messaggi), finalizzate all'esercizio del diritto di difesa, ancora in possesso dell'indagato e non ancora inviati al difensore. Le perplessità derivano a maggior ragione sui messaggi inviati dal difensore all'indagato, dal momento che le garanzie di libertà del difensore fanno riferimento ad attività di ricerca di documenti che si trovano presso lo studio del difensore (art. 103 c.p.p.).

Per via interpretativa, invece, l'ampio divieto su « ogni forma di controllo della corrispondenza », a tutela della "segretezza" (riservatezza) dello scambio informativo fra difeso e difensore, in ragione dell'espletamento della funzione difensiva, dovrebbe estendersi oltre i confini logistici¹², fermo restando che non sempre è agevole individuare a monte la tipologia di corrispondenza, se non dopo l'analisi selettiva degli stessi successiva al sequestro del materiale informatico. Dunque, la sanzione dell'inutilizzabilità dei risultati conseguiti in violazione dei divieti (art. 103 comma 7 c.p.p.), in un contesto così delicato, gioca a valle un ruolo centrale a garanzia dei diritti fondamentali.

3. Acquisizione del documento informatico: profili critici.

La Corte di cassazione ha affermato come l'attività di analisi per la selezione dei documenti richieda del tempo, non potendo i soggetti di polizia giudiziaria effettuare sempre un'estrazione di copia di quelli rilevanti al momento del sequestro, in quanto l'oggetto informatico è complesso da valutare, anche sotto il profilo dei dati utili all'accertamento. Sicché è fondamentale rispettare la disciplina che mira a proteggere, nell'interesse di tutte le parti, l'integrità e affidabilità dei dati informatici acquisiti con la c.d. copia conforme.

Il documento informatico, infatti, implica l'adozione di tecniche peculiari volte a reperirlo, che devono necessariamente tener conto della sua fragilità, essendo lo stesso suscettibile di alterazioni o danneggiamenti (anche involontari: si pensi ad una operazione messa in atto da un soggetto non adeguatamente preparato da un punto di vista tecnico).

¹² G. FRIGO, *Difensore*, in *Commentario del nuovo codice di procedura penale*, diretto da Amodio-Dominioni, Milano, 1989, 667, sul punto si evidenzia come la tutela si estende alla corrispondenza *in itinere* o comunque fuori dalla disponibilità del difensore; F. M. GRIFANTINI, *Il segreto difensivo nel processo penale*, Torino, 2001, 248, secondo cui « si tutela non solo la libera disponibilità della corrispondenza, ma anche il contenuto della stessa »; F. R. DINACCI, *Le garanzie di libertà del difensore tra tutela costituzionale e difficoltà operative*, in *Dir. pen. e proc.*, 2012, 24, il quale, con lettura ampia della disposizione di cui all'art. 103

comma 6 c.p.p., osserva che non siano sequestrabili neanche gli appunti formati dal difeso e ancora in suo possesso oppure non giunti nelle mani del difensore; in senso diffidente, A. SCALFATI, *Ricerca della prova ed immunità difensive*, Padova, 2001, 203, l'autore esclude dalla tutela la documentazione strutturata dall'imputato per organizzare la difesa e non trasmessa ancora al proprio difensore, in quanto la stessa non si trova "presso" lo studio del difensore. In argomento cfr. Corte cost., 19 giugno 1998, n. 229, in www.cortecostituzionale.it; Cass., Sez. Un., 25 febbraio 2010, Mills, in *Cass. pen.*, 2995.

Su queste basi, si tratta di individuare le modalità per acquisire i dati presenti in un supporto informatico; occorre cioè recuperare gli elementi di prova senza alterare il sistema informatico in cui essi si trovano ¹³.

In questa prospettiva, la legge n. 48 del 2008, di ratifica e di esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23 novembre 2001, prevede alcune cautele; il legislatore ha modificato, infatti, alcune norme del III e del IV libro del codice di procedura penale, in ordine a strumenti d'indagine sui sistemi o programmi informatici e telematici (anche se salvaguardati da misure di sicurezza), al fine di assicurare la conservazione dei dati originali, impedirne l'alterazione nel corso delle operazioni di ricerca delle fonti di prova, garantire la conformità della copia all'originale e l'immodificabilità della stessa (quando si procede ad una duplicazione), dotare di sigilli informatici i documenti ¹⁴.

Tale legge, però, non ha regolamentato nello specifico le operazioni (il metodo) di acquisizione di notizie informatiche, in ragione dei diversi protocolli operanti in materia e della valutazione che questi risultano condizionati da una continua evoluzione tecnologica.

¹³ P. PAULESU, *Art. 354, c.p.p.*, in *Codice di procedura penale commentato*, a cura di Giarda-Spangher, 2010, 4267 ss., sul punto si è osservato come « “le tracce digitali” costituiscono ormai elementi cognitivi di primaria importanza nell'ambito dell'investigazione criminale. Sennonché, si sa che il dato informatico, strutturalmente “im-materiale”, risulta fatalmente esposto ad un elevato rischio di dispersione ed alterazione. Labilità dell'elemento cognitivo, urgenza della sua captazione, non dispersione dello stesso sono tutti fenomeni suscettibili di incoraggiare prassi investigative disinvolute. Donde l'esigenza di predisporre alcuni protocolli operativi preordinati ad assicurare la genuinità e la conservazione della digital evidence ».

¹⁴ Con la legge del 18 marzo 2008 n. 48 il legislatore ha modificato alcune norme del codice di procedura penale, all'art. 244, comma 2, c.p.p. sono state aggiunte le parole: « anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione »; all'art. 247 c.p.p., che concerne casi e forme delle perquisizioni, è stato inserito il comma 1-bis: « Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché 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 »; all'art. 254 c.p.p., riguardante il sequestro di corrispon-

denza, è stato sostituito il primo comma: « 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 »; all'art. 254 c.p.p. è stato sostituito il secondo comma: « 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 »; è stato aggiunto l'art. 254-bis c.p.p.: « 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 »; all'art. 256 c.p.p. che riguarda il dovere delle persone indicate negli artt. 200 e 201 c.p.p. di consegnare immediatamente atti e documenti, sono state aggiunte le parole: « nonché i dati, le informazioni e i

Analizzando le norme modificate con la legge n. 48 del 2008 (artt. 244, 247, 254, 254-bis, 256, 259, 260, 352, 353, 354 c.p.p.) risulta evidente come le attività di indagine degli elementi informatici rientrino nel novero dei mezzi tipici di ricerca, recependone la disciplina: di qui una serie di problemi interpretativi sul piano della tutela dei diritti fondamentali dell'individuo e della qualità del giudizio (affidabilità della prova). Problemi che derivano dalla difficoltà, come si è detto, di disciplinare per legge le procedure acquisitive dei documenti informatici.

Su questo terreno, occorre concentrare l'attenzione sulle modalità di recupero del documento informatico; una volta individuato, sul piano investigativo, il supporto digitale, è infatti necessario procedere preliminarmente all'acquisizione della *bit-stream image*¹⁵, anche nel caso di attivazione di accertamenti urgenti e/o ispezioni, sempreché non occor-

programmi informatici, anche mediante copia di essi su adeguato supporto»; all'art. 259, comma 2, c.p.p. riguardante l'obbligo del custode delle cose sequestrate, è stato aggiunto il periodo « Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria »; all'art. 260, comma 1, in relazione al sigillo delle cose sequestrate con appositi mezzi, sono state inserite le parole: « anche di carattere elettronico o informatico, idoneo a indicare il vincolo imposto a fini di giustizia »; nell'art. 352 c.p.p., che riguarda le perquisizioni a iniziativa della polizia giudiziaria, è stato inserito il comma 1-bis: « Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e 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 »; all'art. 353 c.p.p. che prevede che il pubblico ministero autorizzi la polizia giudiziaria a ricercare notizie utili all'assicurazione delle fonti di prova non solamente con l'immediata apertura dei plichi, ma anche (sono state inserite le parole) con « l'accertamento del contenuto » della corrispondenza informatica; all'art. 354 c.p.p., riguardo « accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro », è stato aggiunto: « In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telesa-

tici, 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 ». In tema cfr. Cass., Sez. un., 20 luglio 2017, n. 40963, in *www.dirittifondamentali.it*, secondo cui in virtù delle disposizioni codicistiche (artt. 244 comma 2, 247 comma 1-bis, 254-bis, 256, 260 comma 2, 354 comma 2 c.p.p.) emerge con evidenza come l'estrazione della copia con modalità tali da assicurare la conformità all'originale e la sua immodificabilità è prevista allo scopo di preservare il dato acquisito isolandolo dal sistema che lo contiene, impedendone la successiva elaborazione, trasformazione o eliminazione, sempre possibile anche senza il diretto intervento di un operatore, ad esempio, se precedentemente programmata.

¹⁵ Cfr. S. ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen e proc.*, 2008, Dossier, *La prova scientifica nel processo penale*, 61, tale creazione viene resa non modificabile mediante determinati meccanismi ed in merito si osserva che « questa fase acquisitiva viene effettuata attraverso la *bit-stream image*, ovvero la realizzazione di una "immagine" bit a bit del contenuto del supporto posto sotto sequestro che consente di operare l'analisi forense su un hard disk praticamente identico all'originale: sia sotto il profilo logico sia sotto quello fisico ». Tali cautele sono importanti al fine di evitare che un successivo accesso ad un file tramite dispositivo (tipo *personal computer*) possa essere modificato; infatti, gli aspetti problematici dell'analisi digitale, che riguarda diverse tipologie di supporti (*computer, smartphone,*

rano diverse ore per effettuare tale operazione, in modo da evitare problematiche sull'alterazione dei dati nella fase di analisi degli stessi ¹⁶.

La predetta acquisizione, ove effettuata in precedenza (ad esempio prima del sequestro), deve avvenire in modo tale da assicurare la massima corrispondenza fra l'originale e la copia ¹⁷.

Nella fase di acquisizione occorre redigere una "relazione tecnica", in modo da consentire alle parti e al giudice di verificare l'ammissibilità, l'utilizzabilità e l'attendibilità della prova. Ecco allora che, in una prospettiva *de iure condendo*, parrebbe necessario introdurre l'obbligo di redigere un verbale, a pena di inutilizzabilità della prova documentale informatica ¹⁸. Tale verbale dovrebbe dar conto di una serie di operazioni: recupero del supporto digitale e analisi del dato digitale, lo stato del dispositivo, l'annotazione del giorno e dell'ora di inizio e di cessazione dell'operazione, nonché i nominativi delle persone che hanno preso parte alle operazioni ¹⁹.

navigatori satellitari, etc.) e di risorse *hardware* o *software* distribuite in remoto (*cloud computing*), dove sono archiviati i dati utili ad un'indagine, si colgono prevalentemente nella fase di ricerca del documento informatico.

¹⁶ Basti pensare che ad oggi i tempi di copia sono di circa 2 giga al minuto, per cui, ad esempio, per un *hard disk* di un *terabyte* saranno necessarie 8 ore circa per effettuare una *bitstream image* (cfr. G. VACIAGO, *Profili processuali delle indagini informatiche*, cit., 648).

¹⁷ G. VACIAGO, *Profili processuali delle indagini informatiche*, cit., 651, sul punto si è osservato come « è evidente che, nel momento stesso in cui venga rispettata la procedura di acquisizione *bitstream* dell'immagine del disco e sia verificata, attraverso il calcolo dell'algoritmo di *hash*, la perfetta identità della copia, non vi sono ragioni per ritenere irripetibile tale accertamento tecnico ». In tale contesto è utile ricordare che secondo un orientamento del giudice di legittimità non possono essere invocate le garanzie previste per gli accertamenti tecnici irripetibili, visto che l'attività di estrazione di copia dei file da un computer non determina la irriproducibilità di informazioni identiche a quelle contenute nell'originale, Cass. pen., sez. III, 24 novembre 2010, in CED, 248767; Cass. pen., sez. I, 25 febbraio 2009, *ivi*, 243495, secondo cui non dà luogo ad accertamento tecnico irripetibile la lettura dell'*hard disk* di un computer sequestrato che è attività di polizia giudiziaria volta, anche con urgenza all'assicurazione delle fonti di prova, Cass. pen., sez. I, 18 febbraio 2009, *ivi*, 243922.

¹⁸ Tale riflessione potrebbe far emergere il discorso sull'utilizzabilità della prova, in assenza della predetta regola (obbligo di redigere il verbale). In dottrina risultano

orientamenti opposti in tema di prova incostituzionale (e prova illecita), da un lato c'è chi sostiene che la mancanza di regole probatorie implica l'utilizzabilità processuale del relativo dato probatorio anche in ragione del rapporto gerarchico tra norma costituzionale e norma ordinaria, F. CORDERO, *Tre studi sulle prove penali*, Milano, 1963, 63 e 149; Id., *Procedura penale*, Milano, 2003, 630 ss.; G. LOZZI, *Lezioni di procedura penale*, Torino, 2004, 226; N. GALANTINI, *Inutilizzabilità*, in *Enc. dir.*, I, Milano, 1997, 700; C. CONTI, *Inutilizzabilità*, in *Enc. giur.*, XVII, Roma, 2004, 9; dall'altro, *contra*, G. RICCIO, *Le perquisizioni nel codice di procedura penale*, Napoli, 1974, 181 ss.; G. PIERRO, *Una nuova specie di invalidità: l'inutilizzabilità degli atti processuali penali*, Napoli, 1992, 172; NOBILI, Art. 191, in *Commentario codice di procedura penale*, a cura di Chiavario, Torino, 1990, 409-413; D. SIRACUSANO, *Le prove*, in *Diritto processuale penale*, Milano, 2004, 343; G. ARICÒ, *Riflessioni in tema di inutilizzabilità delle prove nel nuovo processo penale*, in *Annali dell'istituto giuridico dell'Università di Salerno*, 1993, 28; in quest'ambito si osserva che la prova è inutilizzabile in virtù di un'interpretazione costituzionalmente orientata, A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, 1188; A. VELE, *La problematica utilizzabilità del documento formatosi nell'ambito della procedura concorsuale in tema di dichiarazioni rese dal fallito al curatore fallimentare*, in *Giust. pen.*, 2007, 520 ss.; Id., *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Padova, 2011, 97 ss.

¹⁹ Il legislatore, peraltro, non può prevedere in maniera tassativa specifiche mo-

Un adempimento di questo tipo sarebbe, di fatto, necessario per garantire un efficace controllo a posteriori dell'operato degli inquirenti da parte della difesa e del giudice. In questa prospettiva, ad esempio, la difesa potrebbe affidare ad un proprio consulente tecnico o ad un perito (chiedendone l'ammissione) il compito di verificare se le tecniche di recupero e di analisi informatica abbiano alterato o danneggiato dati; non bisogna dimenticare, appunto, che eventuali alterazioni di dati potrebbero inficiare la fase valutativa del giudice, compromettendone la correttezza. Dal canto suo, lo stesso giudice può disporre una perizia *ex officio* ai sensi dell'art. 507 c.p.p.

In questo quadro, emerge il problema relativo all'affidabilità scientifica delle metodologie volte a recuperare il documento informatico; un'incertezza che presenta significative ricadute sull'inammissibilità dello stesso. A questo proposito vi è chi ritiene che la prova non autenticamente scientifica sia manifestamente irrilevante²⁰, nel senso che la stessa non può avere ingresso nel processo. Si è peraltro consapevoli delle difficoltà che il giudice incontra nel verificare a posteriori la violazione di regole tecniche; di qui la necessità di predisporre linee guida volte ad agevolare il vaglio giurisdizionale²¹.

ANTONIO VELE

dalità tecniche, sia perché soggette a variazioni in forza della natura del dato ricercato e dello stato del dispositivo (spento, acceso, operativo *on line*), sia in forza del progresso tecnologico.

²⁰ F. CAPRIOLI, *La scienza "cattiva maestra": insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, 352.

²¹ A. GRILLO-U.E. MOSCATO, *Riflessioni*

sulla prova informatica, in *Cass. pen.*, 2010, 381, secondo cui la parte interessata dovrebbe segnalare e allegare protocolli, linee guida, regole tecniche comunemente accettate dagli ambienti scientifici, che ritiene siano stati violati nel corso della raccolta della prova e abbiano determinato una qualche distorsione della prova.