DIRITTO PENALE CONTEMPORANEO

ANCORA DUBBI E INCERTEZZE SULL'ACQUISIZIONE DELLA CORRISPONDENZA ELETTRONICA

Cass. pen., sez.VI, 24 febbraio 2015 (dep. 10 giugno 2015), n. 24617, Pres. Milo, Rel. Di Stefano, Ric. Rizzo

di Federico Cerqua

Abstract. *Il contributo prende le mosse dall'osservazione secondo cui il progresso digitale ha introdotto nuove modalità di corrispondenza tra le persone. Sul piano processuale una particolare attenzione viene dedicata nella prassi alla posta digitale, in ragione delle numerose informazioni che le e-mail possono veicolare. L'interprete, tuttavia, deve confrontarsi con un approccio particolarmente conservatore da parte della giurisprudenza di legittimità, che presume di risolvere con le categorie della tradizione i problemi posti dalla forensic computing. Ne discende, pertanto, un quadro quanto mai incerto in cui all'indeterminatezza del dato normativo segue irrimediabilmente l'arretramento delle garanzie difensive.*

1. Premessa: i termini del problema.

Nel definire il *diritto di libertà informatica*, Vittorio Frosini spiegava che esso, oltre a manifestarsi come forma di difesa dell'individuo dall'invadenza del mondo sociale, presenta anche «un aspetto attivo di partecipazione al circuito informativo, e la libertà di custodire la propria riservatezza informatica è divenuta anche la libertà di comunicare ad altri le informazioni trasmissibili per via telematica, cioè la libertà di usufruire delle reti di trasmissioni senza limitazione di frontiere, una libertà di espressione della propria personalità valendosi dei sistemi di comunicazione automatizzata»[1].

Volendo ora trasferire l'autorevole osservazione nel campo del procedimento penale, va rilevano anzitutto che il dato prasseologico conferma la sempre più ampia

[1] FROSINI, *La democrazia nel XXI secolo*, Macerata, 2010, p. 41.

diffusione delle attività investigative dirette ad acquisire quali elementi di prova i dati contenuti negli elaboratori elettronici. Il ricorso alla ricerca della *digital evidence* risulta, infatti, imposto dalla rilevante congerie di dati ed informazioni che vengono scambiate attraverso la comunicazione di posta elettronica.

Com'è stato esattamente osservato, dunque, la prova dell'illecito «finisce sempre più abitualmente con l'annidarsi nel *computer* anche in tutte quelle ipotesi in cui il sistema informatico non costituisce il destinatario dell'offesa o l'elemento costitutivo della fattispecie, né tanto meno il mezzo attraverso cui si è perpetrato l'illecito. L'evidenza digitale può infatti essere determinante oramai in ogni inchiesta criminale, dalle indagini per terrorismo … a quelle per reati associativi o dei 'colletti bianchi'»[2]. In tale prospettiva non può sfuggire allora la rilevanza che ai fini investigativi può assumere l'acquisizione della corrispondenza elettronica, atteso il ruolo fondamentale che lo scambio di e-*mail* ha ormai acquisito in ogni settore della vita umana.

Una recente decisione della Suprema Corte, che può leggersi in allegato, offre quindi all'interprete l'occasione per verificare il grado di elaborazione giurisprudenziale sui temi relativi all'acquisizione della prova digitale. In particolare, può risultare utile verificare se la profilatura degli istituti offerta dalla giurisprudenza di legittimità sia coerente con i profili problematici sollevati in campo processuale dai nuovi strumenti digitali. A tale riguardo e senza voler precorrere le conclusioni, può anticiparsi che gli esiti interpretativi raggiunti dai giudici di legittimità non sembrano essere allineati né con il dato normativo né con i profili tecnologici dei mezzi elettronici.

In breve i fatti che hanno originato la decisione della Suprema Corte. Nel corso delle indagini per accertare la violazione del segreto di ufficio, veniva sequestrato il *personal computer* di un giornalista, non indagato in tale procedimento, al fine di acquisire i messaggi di posta elettronica da cui trarre il nome della "fonte" che aveva riferito al giornalista i fatti oggetto dell'indagine, evitando l'opposizione del segreto, ai sensi dell'art. 200, comma 3, c.p.p.

La Corte di Cassazione con la decisione in commento, pur confermando il provvedimento del tribunale del riesame, ha definito la vicenda secondo diverse coordinate interpretative, impegnandosi in un'ampia ricognizione dell'orizzonte operativo entro cui iscrivere l'acquisizione della posta elettronica da un *personal computer*, attraverso la ricostruzione del mosaico normativo che compone il quadro di riferimento della *parte statica* del procedimento di apprensione delle e-*mail*. Non è invece rientrato nel fuoco dell'analisi svolta dai giudici di legittimità il diverso profilo *dinamico* dell'acquisizione dei flussi di posta elettronica circolanti.

In ogni caso, gli esiti argomentativi cui è pervenuta la Suprema Corte impongono qualche ulteriore riflessione, anche in relazione all'attualità dei temi trattati.

---

[2] LUPÁRIA, *La disciplina processuale e le garanzie difensive*, in Lupária – Ziccardi, *Investigazione penale e tecnologia informatica*, Milano, 2007, p. 130 e s.

2. L'ispezione e la perquisizione del *personal computer*.

L'operazione preliminare compiuta dai giudici di legittimità è consistita nell'esame dei più rilevanti meccanismi procedimentali in tema di sequestro della corrispondenza elettronica, modificati dalla l. 18 marzo 2008, n. 48, con cui il nostro Paese ha ratificato e dato esecuzione alla Convenzione siglata a Budapest sulla criminalità informatica, aperta alla firma degli Stati membri del Consiglio d'Europa e di altri Stati non membri il 23 novembre 2001 ed entrata in vigore il primo luglio 2004, quando è stato raggiunto il numero minimo (cinque) di ratifiche necessarie[3].

Ebbene, le linee di riforma che emergono dal compendio normativo introdotto nel 2008 vanno individuate nella necessità di apprestare significative cautele per la salvaguardia del dato digitale, in ragione della sua natura ontologicamente fragile, alterabile e falsificabile[4], ma sempre nel rispetto delle garanzie processuali. Più precisamente, nel settore dell'accertamento informatico «tendono ad acuirsi le intersezioni, comunque tipiche del diritto delle prove penali, tra il piano della tutela della purezza del dato epistemico e quello della salvaguardia del diritto di difesa, giacché ogni dinamica di raccolta di una *digital evidence* sottende un *periculum* tanto per la prima quanto per la seconda. Del resto, rispetto a contesti che presentano affinità, come appunto l'apprensione dei reperti a fini di profilatura genetica, le criticità appaiono decisamente accresciute, sia per la maggiore attendibilità delle evidenze (a seguito di condotte anche inconsapevoli), sia per una distanza ancor più accentuata tra senso comune e tecnologia per attori e comprimari del rito, sia, infine, per una vastità di approcci sedimentata quanto a teorie e tecniche condivise»[5].

Definite in tal senso le direttrici che segnano il quadrante delle investigazioni informatiche[6], va ulteriormente chiarito che le cadenze dell'attività tecnica diretta a trattare, attraverso sistemi *hardware* e *software*, i dati digitali per finalità investigative e giudiziarie (c.d. *forensic compunting*), possono essere distinte in tre diverse fasi: in primo luogo, devono essere individuati i dati interessanti per l'indagine, in modo da definire il campo della ricerca; successivamente si procede all'acquisizione dei dati mediante il sequestro del supporto contenente le informazioni digitali ovvero

---

[3] Alla Convenzione di Budapest ha fatto seguito il Protocollo addizionale alla *Criminalisation of Acts of Racist and Xenophobic Nature Committed through Computer System*. Per un commento organico alle modifiche introdotte dalla l. n. 48 del 2008, Lupária (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009.

[4] LUPÁRIA, Computer crimes *e procedimento penale*, in Garuti (a cura di), *Modelli differenziati di accertamento*, in Spangher (diretto da), *Trattato di procedura penale*, Vol. VII, Tomo I, Torino, 2011, p. 373.

[5] LUPÁRIA, Computer crimes *e procedimento penale*, cit., p. 374.

[6] Individua la ragione dell'intento legislativo di procedimentalizzazione l'indagine digitale, in chiave di tutela dei contenuti informatici, nella necessità di «interrompere usanze investigative devianti e dimentiche di ogni garanzia sotto i profili della genuinità del risultato e del contraddittorio paritetico», LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in Lupária (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cyber crime, Padova, 2009, p. 141 e s.

attraverso l'estrapolazione e la riproduzione del dato su un supporto idoneo; infine, vengono analizzati i dispositivi digitali acquisiti, per recuperare le informazioni di interesse per le indagini[7].

Il primo passaggio operativo nelle investigazioni funzionali all'acquisizione della corrispondenza elettronica, è quindi rappresentato dall'attività ispettiva del sistema informatico. Nel corso di questo primo "contatto" con l'elaboratore elettronico deve essere evitato che i dati informatici siano alterati dall'attività di chi osserva, con la conseguenza che le operazioni ispettive devono essere svolte, ai sensi dell'art. 244, comma 2, c.p.p., adottando le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Ne deriva, pertanto, che l'ispezione informatica si risolve in un'osservazione del sistema attraverso la descrizione del suo *status* e l'annotazione della eventuale presenza di *software* attivi, nonché periferiche e connessioni[8], con la conseguenza che all'attività di osservazione, descritta nel verbale contestualmente redatto, non può seguire quindi alcuna forma di apprensione della posta elettronica eventualmente individuata all'interno del sistema[9]: l'ispezione del sistema, infatti, rappresenta un'attività preliminare rispetto al contesto dell'indagine informatica, «usualmente deputata all'estrazione di dati digitali, pur nelle forme della *legal imaging* generalmente condivisa»[10]. In tale prospettiva, quindi, assumono rilevanza le modalità di perquisizione dell'elaboratore elettronico, dettate dal comma 1-*bis* dell'art. 247 c.p.p., cui fa da *pendant* l'art. 352, comma 1-*bis*, c.p.p.

In particolare, ai sensi della prima disposizione, viene stabilito che l'autorità giudiziaria può procedere alla perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, quando vi sia 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. Il comma 1-*bis* dell'art. 352 c.p.p., precisa inoltre che nelle ipotesi di flagranza del reato ovvero nei casi disciplinati dall'art. 352, comma 2, c.p.p., gli ufficiali di polizia giudiziaria, adottando le misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, possono

---

[7] FELICIONI, *Le ispezioni e le perquisizioni*, in Ubertis – Voena (diretto da), *Trattato di procedura penale*, XX, II ed., Milano, 2012, p. 238 ss., la quale osserva altresì, p. 239 e s., che «in concreto, inoltre, si può determinare una contrazione delle fasi di acquisizione e analisi in un unico momento: si pone la questione dell'analisi immediata (*live data forensics*) che viene effettuata qualora le macchine siano accese. L'analisi, dunque, viene svolta sul luogo al fine di evitare la dispersione definitiva di dati che può essere causata dallo spegnimento del *computer*»

[8] PITTIRUTI, *Profili processuali della prova informatica*, in Marafioti – Paolozzi (a cura di), *'Incontri ravvicinati' con la prova penale. Un anno di seminari a Roma Tre*, Torino, 2014, p. 55 e s.

[9] FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 240; nello stesso senso BRAGHO', *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in Lupária (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cyber crime, cit., p. 195.

[10] MANCUSO, *L'acquisizione di contenuti* e-mail, in Scalfati (a cura di), *Le indagini atipiche*, Torino, 2014, p. 72.

procedere alla perquisizione dei 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 possano essere cancellati o dispersi.

Il legislatore del 2008, recependo la Convenzione di Budapest ha chiaramente distinto tra l'apprensione del singolo dato informatico (il *contenuto*) ed il *personal computer* (il *contenitore*), stabilendo che per l'autorità giudiziaria non è possibile acquisire in modo indiscriminato un intero archivio elettronico, sulla scorta della facilità di accesso al sistema, che consenta di effettuare agevolmente la copia ed il trasferimento fisico dei dati rispetto alla massa di documenti cartacei corrispondenti. Al contrario, l'acquisizione attraverso il sequestro dell'intero *personal computer*, che va comunque disposta nel rispetto del principio di proporzionalità applicabile anche ai mezzi di cautela reale[11], deve considerarsi un'ipotesi residuale che può essere impiegata ad esempio nei casi in cui il *computer* viene impiegato esclusivamente per l'archiviazione di materiale illecito.

3. Le *e-mail* quali documenti digitali.

L'ulteriore aspetto interpretativo che merita di essere affrontato attiene alla qualificazione giuridica della posta elettronica: in altri termini, risulta preliminarmente necessario definire la categoria processuale entro cui condurre le *e-mail*, al fine di meglio precisare i contorni degli istituti coinvolti nelle operazioni di apprensione dei biglietti di posta elettronica.

Ebbene, appare corretto ritenere che ogni comunicazione elettronica, inviata dal *server* alla casella di posta elettronica, costituisca un documento digitale autonomo, che può essere letto nella rete *Internet* attraverso un accesso remoto ovvero "scaricato" sul *personal computer*; inoltre, «ad ogni invio, risposta o inoltro operato dall'utente destinatario del messaggio, il documento originariamente ricevuto muta – anche solo marginalmente – la sua *facies*, generando un nuovo documento che presenta dati esterni identificativi nuovi e distinti, oltre che contenuto informativo solo in parte coincidente»[12].

Con riguardo alla morfologia del documento digitale, può dunque affermarsi che con l'avvento della cosiddetta *Computer Mediated Communication* il testo, «un tempo chiuso nella sua staticità, ha aperto i propri confini a un meta-testo illimitato»[13]: nelle *e-mail* la pratica della citazione (*quoting*) consente di modulare il testo di partenza in

---

[11] La necessità di rispettare il principio di proporzionalità, *ex* art. 275 c.p.p., anche nell'applicazione dei mezzi di cautela reale viene costantemente affermato dalla giurisprudenza di legittimità; sul punto, tra le altre, Cass. pen., sez. III, 7 maggio 2014, Konovalov, in *C.E.D.* n. 261509; Cass. pen., sez. V, 16 gennaio 2013, Caruso, in *C.E.D.* n. 254712; Cass. pen., sez. III, 15 dicembre 2011, Sartori, in *C.E.D.* n. 252223.

[12] MANCUSO, *L'acquisizione di contenuti* e-mail, cit., p. 57.

[13] Per questa e per la citazione immediatamente successiva, PISTOLESI, *Il parlar spedito. L'italiano di* chat, e-mail *e* SMS, Padova, 2004, p. 17 e s.

turni conversazionali, con la conseguenza che il testo è intrinsecamente *aperto*, in quanto ogni messaggio, «diventa un turno che attende il suo completamento nella mossa successiva dell'interlocutore».

La Corte di Cassazione con la decisione in commento ha assegnato al dato informatico un «valore pienamente assimilabile a quello di un oggetto fisico». In tale prospettiva, dunque, i giudici di legittimità confermano l'indicazione fornita dalla dottrina, secondo cui dal punto di vista giuridico «ciò che costituisce il documento è, anzitutto, la cosa che incorpora i segni (*aliquid*) e che può essere del materiale più diverso: pietra, tavole cerate, nastro magnetofonico, pellicola cinematografica o fotografica (in negativo o a stampa) e simili, sino alle odierne memorie informatiche e elettroniche»[14].

La conseguenza più evidente delle conclusioni raggiunte consiste nella possibilità di ricondurre le *e-mail* nella categoria dei documenti alla stessa stregua della posta tradizionale. L'elemento distintivo tra le due categorie documentali è rappresentato piuttosto dalla separabilità del contenuto rappresentativo[15] dal supporto su cui è stato originariamente impresso e, quindi, nella sua modificabilità. In altri termini, nel documento tradizionale «la rappresentazione è *incorporata* in modo inscindibile nella *res* che la memorizza e conserva e ogni copia sarà sempre qualcosa d'altro rispetto all'originale. La *digital evidence*, al contrario, non è vincolata a un determinato contenitore e può essere trasferita da un supporto ad un altro senza perdere alcuna delle proprie caratteristiche e senza subire alcuna modificazione: in sostanza, è duplicabile una serie infinita di volte, senza differenza qualitative dall'originale»[16].

4. L'acquisizione della corrispondenza elettronica.

Nella prospettiva della ricerca di un bilanciamento tra le esigenze investigative e le garanzie di difesa, i maggiori quesiti interpretativi sono posti dalle modalità di acquisizione della posta elettronica.

In particolare, la definizione normativa della percorso acquisitivo delle e-mail, pur non appartenendo al novero delle prove atipiche[17], rappresenta il punto di emersione del più ampio aspetto relativo alla tempestività degli interventi legislativi rispetto all'insorgere di questioni legate all'attualità del progresso scientifico.

---

[14] ZACCHE', *La prova documentale*, in Ubertis – Voena (diretto da), *Trattato di procedura penale*, XIX, 2012, p. 8.

[15] MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2012, p. 701.

[16] ZACCHE', *La prova documentale*, cit., p. 35.

[17] MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4510; FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 39; MANCUSO, *L'acquisizione di contenuti* e-mail, cit., p. 59; MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, p. 1261; ZACCHE', *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. e giust.*, 2013, n. 4, p. 106.

In tale prospettiva la Corte di Cassazione ha rilevato che l'art. 254, comma 1, c.p.p., facoltizza l'autorità giudiziaria a procedere – presso chi fornisce servizi postali, telegrafici, telematici o di telecomunicazioni – al sequestro degli oggetti di corrispondenza inoltrati per via telematica, quando vi sia il «fondato timore di ritenere che essi siano stati spediti dall'imputato o siano a lui diretti o che, comunque, abbiano una relazione con il reato». Al pari di quanto accade con la corrispondenza tradizionale, inoltre, quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria i biglietti elettronici senza aprirli o alterarli ovvero senza prenderne altrimenti conoscenza. Il successivo art. 254 *bis* c.p.p., appositamente inserito nell'intelaiatura del codice di rito dall'art. 8, comma 5, l. n. 48 del 2008, precisa inoltre che l'autorità giudiziaria, quando dispone il sequestro dei dati informatici detenuti dai fornitori di servizi informatici, telematici o di telecomunicazioni, può stabilire per esigenze legate alla regolare fornitura dei servizi medesimi, 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. La disciplina è completata dall'artt. 353, comma 3, c.p.p., dedicato all'acquisizione della corrispondenza tradizionale, così come modificato dall'interpolazione dell'art. 9, comma 2, lett. *a)*, l. n. 48 del 2008. La norma *de qua* stabilisce, quindi, che in attesa del provvedimento di sequestro del pubblico ministero, gli ufficiali di polizia giudiziaria ordinano a chi è preposto al servizio postale, telegrafico, telematico o di telecomunicazione di sospendere l'inoltro degli oggetti di corrispondenza in forma elettronica, ad esempio un plico contenente un *floppy disk*[18], o inviati per via telematica. In quest'ultimo caso – nonostante la velocità di trasmissione dei dati all'interno della rete *Internet* – la polizia giudiziaria è autorizzata a effettuare un fermo posta delle *e-mail*[19], per cui siano registrate necessità di acquisizioni.

Si innesta poi nel percorso normativo dedicato all'acquisizione della posta elettronica il quesito sollevato dalla Corte di cassazione e diretto ad indagare se l'estrazione di copia del dato informatico comporti una perdurante perdita di un diritto sul *personal computer* oggetto delle operazioni di estrazione dei *file*.

I giudici di legittimità hanno risposto al quesito, evocando il disposto dell'art. 258 c.p.p. ed affermando che la restituzione degli atti originali, cartacei o digitali, «previa estrazione di copie, comporti il venir meno del sequestro solo laddove permanga una perdita valutabile per il titolare del bene originale. Perdita che deve essere considerata sul piano di un diritto sostanziale e non deve invece essere considerata quanto al semplice interesse a che la data cosa non faccia parte del materiale probatorio».

---

[18] L'esempio è fornito da ZACCHE', *L'acquisizione della posta elettronica nel processo penale*, cit., p. 108.

[19] Sul tema, tra gli altri, MACRILLO', *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. Internet*, p. 513; VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, in Lupária (a cura di), Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, p. 111 e s.

La prospettiva indicata dai giudici di legittimità merita, invero, alcune precisazioni.

Dal punto di vista della ricostruzione normativa sembra più corretto richiamare l'art. 260, comma 2, c.p.p., così come modificato dall'art. 8, comma 8, lett. *b)*, l. n. 48 del 2008. Secondo la disposizione in esame, infatti, quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria del giudice procedente o dalla segreteria del pubblico ministero.

Ne deriva, dunque, che il testo dell'art. 260, comma 2, c.p.p., rimodulato dalla l. n. 48 del 2008, permette la realizzazione di copie secondo modalità tali da assicurare la loro conformità agli originali ed impedire che il documento digitale si modifichi in seguito alle operazioni di estrazione, in ossequio al rilievo per cui l'attività di acquisizione di copie e di conservazione dei dati digitali, pur non rientrando tra gli atti irripetibili[20], esige delle particolari cautele tecniche, che devono essere adottate in conformità alle *best practies* della *computer forensics*: la volatilità dei dati informatici può essere infatti conseguita solamente evitando il ricorso a condotte non sufficientemente professionali[21]. In tale prospettiva, accanto alla semplice copia clone dei *file*, funzionale ad ottenere la realizzazione della *cluster copy*, può essere ottenuta la *beat stream imagine* o *mirror image*, che rappresenta un esatto duplicato non solo dei *file* – compresi quelli danneggiati o i loro frammenti – ma anche di ogni *bit*. *La bit stream imagine*, peraltro, consente la ripetibilità dell'atto di acquisizione probatoria, permettendo più analisi sullo stesso supporto. D'altra parte, la *bit stream imagine* riduce la durata dell'indisponibilità del bene, consentendo all'interessato di tornare in possesso del *personal computer* subito dopo la conclusione dei lavori di copiatura da parte dell'autorità giudiziaria[22]. Quanto alla verifica dell'assoluta conformità della copia all'originale, «si ricorre generalmente, per motivi di sicurezza, alla funzione matematica *hash*, e cioè ad una funzione non reversibile, in grado di trasformare un dato informatico in una stringa di lunghezza fissa. L'*hash* rappresenta l''imponta' del dato, in quanto se si effettua l'algoritmo su un dato modificato anche solo parzialmente (al limite anche una sola virgola nel contesto di un intero *hard disk*) si ottiene un *message digest* del tutto differente rispetto all'originale»[23]. Per ottenere, inoltre,

---

[20] Cass. pen., sez. I, 5 marzo 2009, n. 14511, in *Cass. pen.*, 2010, p. 1520 con nota di LORENZETTO, *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenitore al contenuto passando per la copia*.

[21] RIVELLO, *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 2013, p. 1716, che esemplificativamente stigmatizza le ipotesi in cui viene inavvertitamente spento un *computer* acceso, operativo o in *stand by*, posto sulla scena del crimine, con conseguente perdita delle informazioni allocate sulla memoria RAM.

[22] LOGLI, *Sequestro probatorio di un* personal computer. *Misure* ad explorandum *e tutele della corrispondenza elettronica*, in *Cass. pen.*, 2008, p. 2955 ss. In argomento, altresì, ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955 ss.

[23] Per questa e per la citazione immediatamente successiva, RIVELLO, *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 2013, p. 1716 ed in particolare nota 117.

l'immodificabilità del supporto di memoria si ricorre generalmente ad un *write blocker*, «volto ad evitare la possibilità di sovrascritture e dunque ad impedire la modifica dei dati».

5. L'utilizzabilità della posta elettronica acquisita.

Durante la fase di acquisizione dei messaggi di posta elettronica riveste, dunque, una primaria importanza l'assicurazione della loro genuinità ed integrità, il cui mancato rispetto si traduce nella inattendibilità e, in definitiva, nella inutilizzabilità del materiale probatorio raccolto.

La decisione in commento, tuttavia, pur richiamando le modifiche innestate nel codice di rito dalla l. n. 48 del 2008, oblitera qualsiasi riferimento espresso alla questione, introdotta dalla *digital evidence*, della qualificazione giuridica delle operazioni di estrazione di copia dei dati informatici dall'elaboratore in sequestro, mostrando comunque di conformarsi all'orientamento proposto dalla giurisprudenza di legittimità secondo cui nell'intento del legislatore del 2008 l'acquisizione dei dati digitali, quindi anche della posta elettronica, mediante l'estrazione di copia dei *file* dall'elaboratore elettronico deve essere ricondotta nell'ambito delle ordinarie attività investigative svolte dalla polizia giudiziaria, quali rilievi, accertamenti urgenti, perquisizioni, ispezioni e sequestri.

In effetti, la Suprema Corte ha affermato più volte che l'attività di estrazione di un *file* non costituisce «atto irripetibile, dato che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare un pregiudizio alla genuinità del contributo conoscitivo in prospettiva dibattimentale. E' assicurata, infatti, in ogni caso, la riconducibilità di informazioni identiche a quelle contenute nell'originale»[24].

Secondo una diversa impostazione, che valorizza la dimensione ontologica del documento elettronico, la natura "volatile" e alterabile propria del dato digitale,

---

[24] Cass. pen., sez. I, 9 marzo 2011, n. 17244, in *Cass. pen.*, 2012, con nota critica di DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*; Cass. pen., sez. III, 24 novembre 2010, n. 45571, in *C.E.D.* n. 243758; Cass. pen., sez. un., 25 febbraio 2010, n. 15208, in *Cass. pen.*, 2010, p. 2995, con nota di FERRARI, *La corruzione susseguente in atti giudiziari, un difficile connubio tra dolo generico e dolo specifico*; Cass. pen., sez. I, 2 aprile 2009, n. 14511, in *Dir. pen. proc.*, 2009, p. 705, con nota critica di RICCI, Digital evidence *e irripetibilità delle operazioni acquisitive*; nonché in *Cass. pen.*, 2010, p. 1520, con nota critica di LORENZETTO, *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenitore al contenuto passando per la copia*. Deve essere inoltre ricordato che le Sezioni Unite della cassazione avevano distinto l'acquisizione di dati digitali mediante estrazione in copia dal provvedimento di sequestro del documento informatico o del computer, in Cass. pen., sez. un., 7 maggio 2008, T.A., in *Dir. pen. proc.*, 2009, p. 469. L'opzione interpretativa è condivisa, tra gli altri, anche da MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, p. 1259 ss., che osserva un duplice vantaggio offerto dall'indirizzo interpretativo in esame: da un lato, verrebbe valorizzato nella sede delle indagini preliminari il suolo *adversary* delle parti, «assicurando, al contempo, l'efficacia e la speditezza dell'azione investigativa; per altro verso, quello di favorire la separazione delle fasi, restituendo al dibattimento la funzione di sede privilegiata della formazione orale della prova nel contraddittorio tra le parti di fronte al giudice», p. 1269.

impone di ricondurre l'attività in esame nell'istituto dell'accertamento tecnico irripetibile. L'esigenza di una tempestiva acquisizione del biglietto di posta elettronica connessa alla natura altamente specialistica delle attività di *digital forensic*, costituirebbero, infatti, indici a favore della natura di accertamento tecnico non ripetibile, «da attivare nei limiti del possibile, e salvo l'effettivo pregiudizio investigativo, nelle forme degli artt. 359 e 360 c.p.p., con l'ausilio di un tecnico qualificato che assuma la piena responsabilità dell'atto di ricerca della prova delegato»[25].

L'indirizzo interpretativo segnalato prende le mosse dal rilievo per cui le indagini informatiche possono mutare il dato digitale[26], con la conseguenza che lo strumento dell'accertamento tecnico irripetibile può consentire di evitare che le prove digitali siano contraffatte o manipolate, richiedendo l'intervento di tecnici specializzati[27].

L'opzione interpretativa in esame, inoltre, sembra meritare apprezzamento, poiché richiede un'anticipazione del contraddittorio nella fase acquisitiva del dato digitale[28], che si mostra – come accennato – particolarmente delicata in quanto è in grado di condizionare le successive fasi di analisi e di valutazione, che altrimenti si fonderebbero su risultati non attendibili[29]. D'altra parte, l'unico limite che potrebbe trovare la ricostruzione proposta attiene all'eventualità in cui il preavviso, imposto dall'art. 360 c.p.p., rischi di vanificare le indagini: si pensi all'ipotesi in cui i dati digitali rimangano a disposizione dell'indagato attraverso il *cloud computing*[30], ovvero i

---

[25] MANCUSO, *L'acquisizione di contenuti* e-mail, cit., p. 65; nello stesso senso, tra gli altri, CURTOTTI, *Rilievi e accertamenti tecnici*, Padova, 2013, p. 183.

[26] Secondo DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, cit., p. 443, «è ancora da dimostrare, in realtà, che le indagini informatiche si possano svolgere senza mutare l'oggetto sui cui cadono, così come vorrebbe il legislatore».

[27] DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 294.

[28] E' stato rilevato che, per evitare il pericolo che l'organo giurisdizionale perda il proprio fondamentale ruolo di "gestione" e di valutazione della prova, deve essere sviluppato al massimo grado il contraddittorio, in modo da sopperire al *gap* conoscitivo del giudice rispetto ai soggetti esperti. Attraverso il contraddittorio, infatti, «è possibile sondare l'effettiva validità delle ipotesi ricostruttive prospettate dalle parti, fornendo al giudice gli elementi necessari per scegliere, fra le varie teorie esposte, quella meglio in grado di fornire una risposta soddisfacente agli accadimenti verificatisi. E' ovvio che pure il ruolo del contraddittorio in materia sia destinato ad essere correlativamente ripensato. Nella gran parte dei casi, infatti, si potrà tradurre al massimo in un contributo dialettico finalizzato alla formazione di un "giudizio "postumo" di idoneità del *modus operandi*, trattandosi magari del reflusso in sede dibattimentale degli esiti di un accertamento tecnico irripetibile», così MARAFIOTI, Digital evidence *e processo penale*, cit., p. 4512 e s.

[29] GARBOLINO, *Nuovi strumenti logici e informatici per il ragionamento giudiziari: le reti baynesiane*, in *Cass. pen.*, 2007, p. 339; FELICIONI, *Ispezioni e perquisizioni*, cit., p. 244 e s., che tuttavia conclude per la necessità di un intervento legislativo «che delinei un autonomo schema procedimentale con garanzie analoghe a quelle che assistono l'accertamento tecnico irripetibile in attuazione del contraddittorio durante l'acquisizione dei dati informatici, a meno che non si ritenga che la cornice della perquisizione entro cui collocare l'estrazione di copia dei dati digitali, sia di per sé sufficiente a garantire sia le ragioni della difesa, sia l'esigenza gnoseologica di un corretto accertamento: in tale ultimo caso, peraltro, il contraddittorio si esplica nella forma di una verifica postuma sulla correttezza dell'indagine informatica».

[30] DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, cit., p. 443.

messaggi di posta elettronica di interesse per l'indagine siano modificabili dall'indagato via *webmail* o con programmi idonei.

Si può allora prospettare un modello operativo "dinamico", che consenta di valutare caso per caso la possibilità di ricorrere all'istituto[31], *ex* art. 360 c.p.p., attraverso soluzioni elastiche, «da modulare sull'esito della verifica differita circa la tecnica di riproduzione digitale adottata dall'investigatore, poiché soltanto una modifica irreversibile del dato estrapolato avrebbe richiesto la compartecipazione preventiva al compimento dell'atto»[32].

6. Conclusioni. Difficoltà di aggiornamento e aporie del sistema: la possibile violazione del segreto epistolare.

Un ulteriore aspetto sollevato dalla possibilità di acquisizione della posta elettronica, che però non è stato oggetto di specifica riflessione da parte della Suprema Corte nella decisione in esame attiene alla tutela del segreto epistolare, garantita dall'art. 15 Cost. e 8 CEDU.

Con particolare riferimento al diritto di segretezza delle fonti riconosciuto al giornalista dall'art. 200 c.p.p., i giudici di legittimità nella sentenza in commento hanno ritenuto che il ricorso alla perquisizione e al sequestro della posta elettronica per acquisire il nome della "fonte giornalistica" non è consentito, salvo che non ricorrano, *ex ante*, le condizioni per escludere l'operatività del diritto al segreto.

Allargando il grandangolo dell'osservazione al diritto di tutela del segreto epistolare, appare opportuna qualche ulteriore osservazione in relazione alle diverse modalità acquisitive del biglietto di posta elettronica.

Nell'ipotesi, invero, in cui si proceda all'acquisizione delle missive elettroniche dall'ente gestore, secondo il dettato degli artt. 254 e 254 *bis* c.p.p., la corrispondenza non può essere né alterata né letta, con la conseguenza che non si verificano lesioni al diritto della segretezza delle comunicazioni.

Maggiori criticità si registrano, invece, nell'ipotesi in cui l'attività di apprensione avvenga attraverso le regole ordinarie in tema di sequestro, che consentono alla polizia giudiziaria di agire di propria iniziativa, ispezionando i messaggi elettronici ed acquisendoli. In tali ipotesi, quindi, si registra una palese violazione delle garanzie riconosciute dall'art. 15 Cost., che si estendono anche in un momento successivo all'apertura del piego – sia esso anche di natura elettronica – da parte del destinatario, e che non prevedono alcuna eccezione alla necessità di un atto motivato da parte dell'autorità giudiziaria.

Ne deriva, pertanto, che se il segreto epistolare può cedere il passo solamente «quando la missiva perde il valore di comunicazione attuale, per acquisire un

---

[31] LUPÁRIA, *La disciplina processuale e le garanzie difensive*, cit., p. 154.

[32] LORENZETTO, *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenitore al contenuto passando per la copia*, cit., p. 1533.

significato meramente retrospettivo, affettivo, storico ecc., ciò significa che la posta elettronica già letta e archiviata dal destinatario nell'apposita cartella, finché attuale, risulta coperta dall'art. 15 Cost. e, come tale, andrebbe assunta»[33].

In conclusione, il nitore del dato normativo, innovato dalla novella del 2008, appare più virtuale che reale e le indicazioni interpretative fornite dalla giurisprudenza – improntate ad un approccio che pretende di risolvere attraverso le categorie tradizionali i problemi posti dalle nuove tecnologie – non sembrano fornire all'interprete gli strumenti utili per affrontare compiutamente le questioni introdotte nel campo processuale dalla *digital evidence*.

[33] ZACCHE', *L'acquisizione della posta elettronica nel processo penale*, cit., p. 110, il quale rileva una possibile illegittimità costituzionale dell'art. 354, comma 2, c.p.p., poiché in assenza di un'autorizzazione preventiva dell'autorità giudiziaria, non dovrebbe essere consentito alla polizia di procedere all'apprensione mediante sequestro della corrispondenza elettronica né tantomeno accedere alla relativa casella. Osserva, altresì, LUPÁRIA, *La disciplina processuale e le garanzie difensive*, cit., p. 172 e s., che, la valutazione va compiuta caso per caso, a seconda delle numerose forme di corrispondenza telematica differenti dal "classico" messaggio di posta elettronica, anche se, salvo alcune ipotesi (il messaggio scaricato, aperto e letto con un programma del tipo di *Outlook Express*), «sembra maggiormente corretto procedere per una qualificazione dell'*e-mail* in termini di posta chiusa».