IL FORO MALATESTIANO

L'UTILIZZO PROCESSUALE DI SMS: L'INTRINSECA INAFFIDABILITÀ DEL DATO INFORMATICO MINA LA VALENZA PROBATORIA DELL'ACQUISIZIONE MEDIANTE RIPRODUZIONI FOTOGRAFICHE

Donato Eugenio Caccavella e Marco Rossi ([1])

1. PREMESSA

Con la sentenza annotata ([2]), il Tribunale di Pesaro affronta un tema a volte trascurato nelle aule di giustizia ossia la utilizzabilità e la valenza dimostrativa delle riproduzioni fotografiche di SMS.

Nel caso di specie i messaggi erano stati inviati dall'imputato alla persona offesa e contenevano le minacce medianti le quali sarebbe stato perpetrato il delitto di estorsione. L'acquisizione degli SMS non avveniva ad opera della polizia giudiziaria, bensì attraverso le fotografie scattate dalla vittima al *display* del cellulare, rimasto sempre nella disponibilità dell'offeso.

Il Giudice pesarese non nega l'utilizzabilità della prova documentale così entrata nel processo, tuttavia afferma che l'acquisizione della mera riproduzione fotografica del *display* non fornisce quelle garanzie di affidabilità che possono provenire esclusivamente dall'esame fisico, secondo le regole del codice di rito, del supporto contenente i messaggi. Pertanto, in assenza di tali garanzie, la forza dimostrativa del documento è inscindibilmente legata all'attendibilità e all'affidabilità del soggetto dichiarante. Orbene, nel caso concreto, stante il giudizio di inaffidabilità della persona offesa operato dal giudice nella sentenza, anche le fotografie degli SMS da lei prodotte finiscono per subire la medesima sorte, con conseguente mancanza della prova delle minacce estorsive.

[1] I paragrafi 1 e 3 sono stati curati da Marco Rossi; il paragrafo 2 è stato curato da Donato Eugenio Caccavella.

[2] La sentenza annotata del Tribunale di Pesaro in data 23 gennaio 2018, depositata il 19 marzo 2018 è pubblicata su questo numero nella sezione "Giurisprudenza".

Il Tribunale dei Pesaro perviene a questa decisione dopo aver preso in esame la consulenza tecnica della difesa che ha evidenziato come la mancata acquisizione agli atti del telefono cellulare si sia risolta in una rilevante carenza istruttoria, posto che soltanto l'esame dello stesso, mediante accertamento tecnico irripetibile, avrebbe potuto fornire adeguati chiarimenti in merito alla genuinità dei dati contenuti negli SMS, portati, invece, nel processo solo mediante riproduzione fotografica.
Stante l'importanza che ha assunto nel processo *de quo*, l'esame e l'elaborato del consulente, occorrerà necessariamente prendere in considerazioni le sue valutazioni tecniche che illustrano le ragioni dell'insita inaffidabilità del dato informatico e le modalità della sua corretta acquisizione, onde poi ricostruire la disciplina applicabile al caso concreto.

2.1. SULLA ATTENDIBILITÀ DEGLI SMS. IL DATO INFORMATICO

Il dato informatico non è altro che una successione di *bit*, cioè di 0 e di 1, registrati all'interno di un dispositivo. Tale dispositivo può essere di qualsiasi natura e può utilizzare qualunque tipo di tecnologia; significativo è, tuttavia, il rilievo per cui il dato digitale è comunque riconducibile ad una successione di 0 e di 1, che, a seconda del supporto su cui sono registrati, vengono rappresentati in modalità diversa: per esemplificare, è possibile immaginare che alla parola "ciao" corrisponda una definita successione di zero e di 1, come ad es. 01000100101001001010101111100101. Paradossalmente, lo stesso dato informatico stampato su un foglio di carta ricalca comunque detta successione, rappresentata dai simboli riprodotti sul supporto cartaceo utilizzando la codifica ASCII – che associa ad una precisa successione di 0 e di 1 un simbolo da riprodurre sul supporto cartaceo – o altra codifica.
Occorre altresì considerare una precedente registrazione di *bit* su un dispositivo, il cui stato, impartendo opportuni comandi, possa essere stato modificato da un operatore.
Infatti, allorché venga generata la successione di *bit*, sussiste la possibilità che almeno un operatore possa in un preciso momento modificarne la successione: per esempio, in un sistema informatico su cui è installato un sistema operativo che preveda la figura di amministratore, chiunque sia a conoscenza della *password* di amministratore può in qualsiasi momento modificare qualunque *file* contenuto nel sistema.
Ugualmente, nel caso di *bit* registrati su supporti non scrivibili, una modifica è sempre possibile, atteso che prima che i *bit* vengano registrati sul supporto possono subire alterazioni: viceversa, se una successione di *bit* è registrata su un supporto non riscrivibile, è possibile escludere *a priori* l'eventualità che tale successione sia stata alterata rispetto alla sua versione iniziale.
Inoltre, a rendere ancora più complessa la questione è il rilievo per cui "*analizzando il supporto su cui sono registrati i bit, non è possibile accertare ed individuare eventuali modifiche apportate in precedenza ai singoli bit"*, non consentendo la

successione di *bit* di capire se gli stessi in precedenza abbiano assunto valori diversi in seguito modificati.
Un esempio che potrebbe concretare il concetto testé esposto è dato da una torcia elettrica, trovata accesa o spenta (*bit* valore 0 o 1): indipendentemente dallo stato in cui è stata rinvenuta, infatti, non è possibile determinare se quello fosse il suo stato originario o se sia stato successivamente modificato. In questo caso, andrà considerata la successione logica dei *bit*, e non eventuali tracce che possono essere presenti a livello fisico sul supporto su cui è registrata detta successione, e che, al contrario, andrebbero ricondotte alla successione in parola.
La possibilità della modifica di una successione di *bit* andrebbe presuntivamente considerata come avvenuta, con la conseguenza che, qualora in un processo venisse prodotto un dato informatico, lo stesso andrebbe presuntivamente considerato come modificato ad arte, dovendo la parte interessata alla sua acquisizione nel *thema probandum* dimostrarne l'attendibilità.
Tuttavia, lo scetticismo non potrebbe spingersi fino ad una dichiarazione di inattendibilità del dato informatico, in quanto tale considerazione verrebbe facilmente contraddetta dall'esistenza della stessa firma digitale.
Ugualmente, la presunzione di ripudio del dato informatico non dovrebbe far pensare che il dato informatico sia inutilmente entrato nel processo, bensì deve essere percepita nel senso che la parte che produce un dato informatico sia onerata dalla dimostrazione della genuinità ed attendibilità del dato stesso, come verrà illustrato successivamente.

2.2. *(segue)*. IL TRATTAMENTO DEL REPERTO INFORMATICO

Ferma restando la volatilità del dato informatico, per dimostrare la non ripudiabilità del reperto prodotto in giudizio, bisogna innanzitutto illustrare le modalità con cui è stato trattato. Per tale attività, sono individuate cinque fasi: l'individuazione, l'acquisizione, l'analisi, la valutazione e la rappresentazione.
L'individuazione del reperto informatico non è un'operazione così semplice come potrebbe a prima vista sembrare, essendo di palmare evidenza che se il reperto non viene prontamente individuato, il medesimo resta esposto per un tempo maggiore al rischio di inquinamento, se non alla sua distruzione vera e propria.
Va ribadito come, stante la diffusione dell'informatica in dispositivi ed apparecchiature anche non tradizionalmente "informatiche" quali il sistema di controllo di una centralina elettronica di un'automobile, o un qualsiasi elettrodomestico "evoluto", ovvero macchine fotografiche digitali – tenendo a mente che, in questo caso, il riferimento non è alle immagini, bensì al concetto *file*, ben potendo, quindi, trovarsi file registrati, tra cui *file* di *word* cifrati con PGP, anche all'interno di una macchina fotografica, o di un telefono cellulare – nella fase di individuazione del reperto informatico vanno singolarmente analizzati gli oggetti individuati, e per ciascuno di essi va verificata l'esistenza o meno di reperti informatici eventualmente registrati su di esso.

In questa fase, vanno intesi come reperti informatici anche documenti stampati, quali un'*e-mail* stampata su un foglio di carta piuttosto che registrata all'interno di un disco rigido. Infine, l'individuazione del reperto informatico deve essere esaustiva ed approfondita, non potendo riguardare solo supporti "informatici", bensì anche altri tipi di supporto, così come vanno osservati una corretta conservazione ed imballaggio del supporto su cui sono registrati i reperti: infatti, in considerazione del reperto, andranno accuratamente scelti gli opportuni contenitori ed anche le modalità di conservazione

Nel caso di un *computer* palmare, per esempio, occorrerebbe conservare lo stesso avendo cura di mantenere sempre alimentate o cariche le batterie, onde evitare che tutti i reperti vengano completamente cancellati; ovvero, nelle ipotesi di supporti rappresentati da *personal computer*, andrebbero alimentate le batterie tampone del BIOS, che tendono a scaricarsi cancellando tutte le impostazioni del BIOS stesso, comportando perdite che, benché minime, potrebbero essere al contrario significative.

La fase di acquisizione del reperto informatico è la più delicata e complessa in assoluto: infatti, se la fase di individuazione dello stesso, per quanto importante, è eseguita in modo scorretto, può accarare che alcuni elementi probatori vadano persi, ma tale dato sarà difficilmente contestato dalla parte che ha interesse alla produzione di tali dati ed alla loro non ortodossa individuazione; al contrario, se è l'acquisizione del reperto ad esser stata eseguita in modo non conforme, sicuramente verrà utilizzato tale argomento per ripudiare il dato acquisito.

La caratteristica essenziale dell'acquisizione consiste nella completezza, essendo stato in precedenza rilevato che il dato informatico non è una successione di *byte*, bensì di *bit*, con la conseguenza che nella fase *de qua* devono essere acquisiti tutti i *bit*.

Pertanto, in questa fase, andranno utilizzati strumenti che, indipendentemente dal tipo di *file system* e dal tipo di tecnologia utilizzata, consentano l'acquisizione dell'intera successione di *bit* presente sul supporto. Inoltre, l'acquisizione del reperto informatico dovrà essere accurata, nel senso che andranno acquisiti unicamente i dati presenti nei vari supporti magnetici, al netto dei componenti *hardware* che non contengano dati informatici, quali, ad esempio *monitor*, *mouse et similia*.

Infatti, nella fase in parola l'oggetto su cui concentrare l'attenzione è il *bit*, ovverosia l'unità atomica di informazione gestita da un *computer*, l'elemento atomico del dato informatico.

Inoltre, nel corso della e dopo la fase *de qua*, e quindi durante la custodia del reperto informatico, andrà impedita qualsivoglia forma di alterazione del reperto, onde evitare di distruggere o modificare elementi di prova ivi contenuti. Pertanto, andranno adottati opportuni strumenti che offrano la garanzia e possibilità di verifica che il reperto informatico sia stato acquisito senza alcuna alterazione, conservando la possibilità di accertamento della corrispondenza esatta fra il supporto di

partenza e quello di arrivo, impropriamente definibili, rispettivamente, originale e copia, atteso che da un punto di vista informatico la copia e l'originale coincidono.
Stante la particolare delicatezza caratterizzante la fase di acquisizione del reperto informatico, unita all'elevata alterabilità del dato informatico, tutte le operazioni di individuazione del reperto informatico andranno accuratamente documentate: al fine di garantire il rispetto dei principi esaminati, l'attività svolta in fase di acquisizione sarà accuratamente documentata, possibilmente utilizzando dispositivi che registrino automaticamente quanto viene eseguito. In questo modo, infatti, sarà conservata traccia di tutte le operazioni compiute, cosa che difficilmente potrebbe accadere se il verbale delle operazioni fosse stato redatto *a posteriori*, atteso che, in questi casi, vengono sintetizzate le attività poste in essere, ma non descritte in maniera dettagliata i singoli comandi battuti; ugualmente, sarà evitato il rischio che, per errore umano, non possa esserci un'esatta corrispondenza tra quanto battuto sulla tastiera e quanto voluto dall'operatore.
Per esemplificare, il comando "cd ." è ben diverso e dal comando "cd ..": per tal motivo è opportuno che le operazioni eseguite in fase di acquisizione del reperto informatico vadano filmate, per quanto riguarda l'accesso al sistema e l'interazione con eventuali interfacce grafiche, così come sarebbe opportuno registrare con appositi dispositivi tutti i tasti battuti sulla tastiera.
Anche durante la fase di analisi del reperto bisogna evitare di alterare il supporto di sorgente, dovendo tutte operazioni di analisi esser eseguite su una o più copie dello stesso, dal momento che la copia coincide con l'originale.
La caratteristica fondamentale della fase di analisi è la riproducibilità delle operazioni eseguite, nel senso che eseguendo operazioni identiche va ottenuto sempre lo stesso risultato. Inoltre, se sono eseguite operazioni logicamente identiche, i risultati devono corrispondere a meno della loro rappresentazione: esemplificando, la consultazione di un documento scritto con un programma di videoscrittura eseguita con lo stesso programma dovrà produrre il medesimo risultato, mentre la consultazione eseguita con un altro programma potrà comunque produrre risultati diversi, tuttavia differenziati fra loro solo per una diversa rappresentazione dello stesso dato, dovendo essere, per esempio, impaginato in maniera diversa.
Questa caratteristica garantisce che, nella dialettica del processo, qualsiasi rilievo sollevato da una parte in merito ad un reperto informatico possa essere verificato anche dalle altre parti.
Preliminarmente, va chiarito il motivo per il quale è necessaria anche una fase di valutazione del reperto, considerato che il *bit* può assumere solo il valore di 0 o 1.
Tale necessità riposa sulla circostanza per cui, potendo il reperto informatico subire alterazioni, inquinamenti, contraffazioni, occorre accertare se si siano verificati questi eventi, se erano potenzialmente verificabili, e chi avrebbe eventualmente potuto

compiere tali operazioni. Inoltre, bisogna accertare se le operazioni di acquisizione del reperto siano state eseguite tecnicamente in modo corretto, nel rispetto della normativa vigente.
Pertanto, valutati ed esposti tali requisiti, vanno formulati giudizi di merito riguardo a due elementi: l'attendibilità del reperto informatico, nel senso della sua integrità, verificando se sia stato più o meno alterato nel tempo; l'autenticità del reperto, consistente nella possibilità di accertarne l'autore o gli autori e con quale grado di sicurezza.

2.3. *(segue)*. L'ATTENDIBILITÀ DEGLI SMS

Sintetizzata la metodologia da osservare in materia di trattamento dei reperti informatici, è opportuno illustrare tecnicamente – con la dovuta comprensibilità per il giurista – le operazioni necessarie per creare o modificare ad arte degli SMS presenti su un dispositivo di telefonia mobile, senza lasciare tracce, in modo da evidenziare l'assoluta inattendibilità di quanto eventualmente riportato nel capo di imputazione.
A tale scopo sarà sufficiente eseguire una ricerca in Internet usando la parola chiave "*fake* sms", ossia "falso sms":
La ricerca genera moltissimi riscontri, indicando il tema suscita interesse; cercando fra la documentazione è possibile individuare, fra i tanti, un sito *web https://www.spoofcard.com/*, che fra le sue funzionalità permette appunto di creare su un dispositivo dei "falsi SMS".
Appare quindi evidente come il contenuto degli SMS non possa di per sé essere considerato attendibile, essendo potendo "creare" ad arte qualsiasi SMS.
Per modificare il contenuto del messaggio riportato andrà cancellato quello originale e creato uno *ex novo* con le stesse caratteristiche temporali e di mittente, ma con il contenuto modificato.
In questa maniera tale "falso SMS" troverà riscontro nei tabulati telefonici, perché andrà a sostituire un SMS effettivamente inviato.
In considerazione della illustrata semplicità e della possibilità da parte di chiunque di modificare ad arte dei messaggi SMS ricevuti, appare evidente come il contenuto degli SMS riportati nella notizia di reato di cui al caso deciso dalla sentenza in commento non possa in alcun modo essere considerato attendibile, atteso che, con le poche e semplici operazioni illustrate, è possibile "modificare" ad arte qualsiasi SMS.
Infatti, nel corso del processo è stato provato come il dispositivo di telefonia mobile fosse nella disponibilità della parte offesa e del tutto privo di una sia pur minima attività di indagine informatica, al contrario doverosa.
Infatti, è notorio che esistano strumenti specifici di acquisizione forense dei dispositivi di telefonia mobile che impediscono o rendono minima l'alterazione del reperto informatico e che vengono specificatamente realizzati per scopi forensi.
Nello specifico, il *National Istitute of Standard and Technology* prevede che per svolgere l'acquisizione dei dati presenti su dispositivi di telefonia mobile vadano rispettati il principio di integrità di quanto acquisito, il

principio di autenticità e di completezza dei dati.
Infatti, la metodologia ed in particolare gli strumenti utilizzati devono garantire che quanto acquisito ed altresì il dispositivo originario non abbiano subito alterazioni, che la copia generata sia equivalente al dispositivo originario e che la stessa sia completa. L'omessa osservanza delle pur brevemente esposte metodologie non assicura la garanzia della bontà di quanto acquisito, nel senso della sua attendibilità.
Il dibattimento ha altresì atto emergere ulteriori carenze metodologiche operate dalla PG, che avrebbe dovuto verificare o acquisire l'intero contenuto del dispositivo in uso alla parte offesa, sussistendo l'obbligo di verificare la natura o meno degli SMS ed eventuali tracce di artefazione dei dati o anche l'individuazione di SMS cancellati.
Esemplificando, l'aver rinvenuto fra gli elementi processuali di prova il solo SMS "ti osservo e ti controllo" acquisirebbe un significato diverso se, al contrario, da una completa verifica il medesimo SMS fosse stato seguito da un altro SMS, contenente la precisazione "naturalmente scherzo".
La parzialità, soggettività e inattendibilità dell'accertamento, inteso come acquisizione solo della rappresentazione di alcuni elementi del reperto e non dell'intero contenuto del cellulare, pregiudica gravemente l'attendibilità e la scientificità dell'accertamento stesso, non potendo detta carenza esser sanabile in una fase successiva al suo trattamento ed al contrario consentendo di verificare la presenza di SMS cancellati o di programmi o tracce di alterazione dolosa dei reperti o la bontà dei messaggi riportati in atti.
Nel caso di specie, quindi, l'accertamento tecnico svolto dalla PG sul dispositivo cellulare della parte offesa avrebbe dovuto esser considerato un accertamento tecnico irripetibile *ex* art. 360 c.p.p., non permettendo le gravi carenze metodologiche l'esecuzione di una serie di accertamenti che avrebbero permesso di verificare la bontà degli SMS presenti sul reperto, rendendo l'accertamento tecnico non attendibile e quindi inutilizzabile.

3. LA DISCIPLINA APPLICABILE

Le osservazioni tecniche appena illustrate, pongono in luce importanti problematiche giuridiche che riguardano gli strumenti normativi più opportuni per la ricerca della prova e per l'acquisizione della stessa[3], quando ha ad oggetto dati informatici[4], senza dimenticare i diritti e le garanzie che debbono essere riservati all'imputato[5].

[3] «La particolarità delle "prove digitali" risiede nel fatto che devono essere raccolte in un luogo virtuale, dove perde consistenza la naturale propensione dell'uomo a rapportarsi con il mondo circostante con l'uso dei sensi e, in particolare, con il tatto»: CUOMO, GIORDANO, *Informatica e processo penale*, in *Proc. pen. e giust.*, 2017, p. 716.

[4] La Convenzione di Budapest definisce dato informatico «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione».

[5] In generale, si può affermare che la *computer forensics* si occupa di individuare corrette procedure di acquisizione della prova informatica e nello specifico delle seguenti attività: «documentazione delle operazioni; individuazione univoca dei file per garantire la non ripudi abilità; corretta conservazione, con particolare attenzione

Il codice di rito, adeguandosi all'importanza che sempre più ha assunto la prova digitale nel processo[6], contiene, da appena un decennio, disposizioni sul tema, introdotte dalla legge n. 48/2008 esecutiva della Convenzione di Budapest (Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2011[7]).

Fra tali norme occorre prendere in considerazione[8] l'art. 247, comma 1-*bis*, c.p.p. in tema di perquisizioni e l'art. 244 c.p.p. in tema di ispezioni. Il minimo comune denominatore delle disposizioni appena richiamate è dato dal fatto che l'autorità giudiziaria quando tratta dati informatici deve adottare misure tecniche che assicurano la conservazione dei dati originali impedendone l'alterazione.

Il Legislatore richiede, quindi, che siano apprestate «significative cautele per la salvaguardia del dato digitale, in ragione della sua natura ontologicamente fragile, alterabile e falsificabile»[9]. Ne consegue che durante l'ispezione, che normalmente rappresenta il primo contatto con il dato informatico, ne deve essere evitata l'alterazione, così come in caso di perquisizione del supporto che, in ipotesi di flagranza di reato o nei casi dell'art. 352, comma 2, c.p.p., può essere eseguita anche dalla polizia giudiziaria[10].

---

a tutta la c.d. catena della custodia; inalterabilità o immodificabilità o verifica della mancata alterazione e della mancata modificazione»: BRAVO, *Indagini informatiche e acquisizione della prova nel processo penale*, in *Rivista di criminologia, vittimologia e sicurezza*, vol. III n. 3, vol IV n. 1, 2009-2010, p. 231. Si veda per un inquadramento ad ampio raggio della disciplina, LUPARIA, ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007.

[6] La prova digitale è definita come il «complesso delle informazioni digitali che sono in grado di stabilire se un crimine è stato commesso o che possono rappresentare un collegamento tra un crimine e suoi esecutori»: CASEY, Digital evidence and computer crime, in Academic Press, 2000, p. 196 ss.

[7] Il testo della Convenzione è consultabile in *www.coe.int*. In generale si veda, COLOMBO, *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali*, in *Ciberspazio e diritto*, 2009, n. 3/4, p. 285 e ss.; CORASANITI, CORRIAS LUCENTI, Cybercrime, *responsabilità degli enti, prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Padova, 2009; CUNIBERTI, GALLUS, MICOZZI, ATERNO, *Commento alla legge di ratifica della convenzione di Budapest del 23 novembre 2001*, in *giuristitelematici.it.*

[8] Di rilievo è anche la norma contenuta nell'art. 254-*bis* c.p.p., sul sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni. A proposto di sequestro, non è applicabile la disciplina dettata dall'art. 254 c.p.p., con riferimento a messaggi rinvenuti in un telefono cellulare, in quanto 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, così, Cass., sez. III, 25 novembre 2015, n. 928, Giorgi, in *C.e.d. Cass.*, n. 265991

[9] CERQUA, *Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica*, in *Dir. pen. cont.*, 23 luglio 2015, p. 3; si veda anche LUPARIA, Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, a cura di Spangher, vol. VII, t. 1, 2011, p. 373.

[10] «L'attività di perquisizione informatica o telematica tende al sequestro delle cose attraverso l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, che concerne la fase di esecuzione della ricerca e dell'ablazione delle informazioni rinvenute all'interno del sistema esplorato»: CUOMO, GIORDANO, *Informatica e processo penale*, cit., p. 718; nonché CISTERNA, *Perquisizioni in caso di fondato motivo. (Legge*

Il codice assegna, nell'ambito della attività d'indagine, alla polizia giudiziaria non solo un potere di conservazione e osservazione ma anche di azione, infatti nei casi di urgenza di cui all'art. 354, comma 2, c.p.p. la polizia giudiziaria ha il compito di provvedere alla duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale[11] e la sua immodificabilità. Ciò che richiede la norma processuale è l'impiego di modalità tecniche, peraltro non tipizzate[12], che assicurino la genuinità[13], rimandando pertanto alla fase istruttoria la valutazione se in concreto vi è stata alterazione dei dati originali e la corrispondenza ad essi di quelli estratti[14]. L'attenzione del Legislatore è cioè volta a far si che durante tutto il procedimento si possa sempre dimostrare che la copia utilizzata in giudizio sia identica a quella originale al momento in cui è stata rinvenuta, ovvero che il dato oggetto di valutazione sia il medesimo di quello acquisito originariamente[15].

Secondo l'opinione giurisprudenziale dominante, l'attività di acquisizione del dato informatico mediante duplicazione, anche al di fuori dei casi di urgenza, non richiede la necessaria costituzione del contraddittorio fra le parti nelle forme dell'art. 360 c.p.p.[16], infatti, «è da escludere che l'attività di estrazione di copia di *file* da un *computer* costituisca un atto irripetibile (…), atteso che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale»[17].

---

18 marzo 2008 n. 48), in *Guida dir.*, 2008, f. 16, p. 66.

[11] La delicatezza dell'operazione tecnica è illustrata da COSTABILE, Computer forensics *e informatica investigativa: profili tecnici di base*, in *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea*, a cura di Cajani, Costabile, Forlì, 2011, p. 131.

[12] Cass., sez. III, 28 maggio 2015, n. 37644, R., in *C.e.d. Cass.*, n. 265180. A tal proposito rileva anche quanto affermato da Cass., sez. Un., 20 luglio 2017, n. 40963, Andreucci, in *C.e.d. Cass.*, n. 270497: «la concreta esecuzione delle attività finalizzate all'acquisizione del dato va calibrata secondo le specifiche esigenze del caso».

[13] Si evidenzia, tuttavia, che il termine "copia" non è del tutto convincente, poiché «potrebbe suggerire eventuali interpretazioni tese a legittimare procedure non rispettose delle migliori soluzioni informatiche in materia, pericolo che una terminologia tecnica più precisa avrebbe evitato»: SENOR, *Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione di Budapest sulla criminalità informatica: modifiche al codice di procedura penale ad al D.Lgs. 196/03*, in *altalex.com, 20* maggio 2008

[14] «Si versa quindi in ipotesi non di inutilizzabilità, ma di valutazione in concreto della prova e quindi, nella specie, dell'eventuale avvenuta o meno alterazione dei dati originali e della corrispondenza o meno di quelli estratti a quelli originali»: Cass., sez. II, 8 luglio 2015, n. 29061, p.c. in proc. Posanzini, in *C.e.d. Cass.*, n. 264572.

[15] Così anche, Cass., sez. VI, 12 febbraio 2014, n. 10618, Genchi, in *C.e.d. Cass.*, n. 259782.

[16] Condivide questa impostazione interpretativa, MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, p. 1259 s.

[17] Cass., sez. I, 2 aprile 2009, n. 14511, in *Dir. pen. proc.*, 2009, p. 705. Nello stesso senso, Cass., sez. II, 1 luglio 2015, n. 29061, cit.; Cass., sez. I, 9 marzo 2011, n. 17244, F.M., in *Cass. pen.*, 2012, p. 440; Cass., sez. III, 24 novembre 2010, n. 45571, Malfanti, in *C.e.d. Cass.*, n. 248767; Cass., sez. I, 30 aprile 2009, n. 23035, Corvino, in *C.e.d. Cass.*, n. 244454.

Tuttavia, si ritiene che la natura facilmente alterabile del dato informatico[18], e l'elevato pericolo che un intervento eseguito in difformità alla *best practice* individuata dalla *digital forensics* possa alterarlo in modo irreparabile e pregiudizievole per il corso del procedimento penale[19], siano elementi che riconducono l'acquisizione del dato informatico all'ipotesi di cui all'art. 117 dispp. att. c.p.p.[20] e pertanto ricadere nell'alveo dell'art. 360 c.p.p.[21] che consente a tutte le parti e alla persona offesa di assistere, mediante preavviso, all'atto con il proprio difensore e con la nomina di un consulente che va ad integrare il contradditorio tecnico sull'acquisizione del dato informatico.

Quella appena illustrata dovrebbe essere la modalità "ordinaria" di acquisizione dell'evidenza informatica, tuttavia non si ignora che molto spesso il preavviso imposto dall'art. 360 c.p.p.[22], potrebbe vanificare le indagini consentendo al soggetto che dispone del dato digitale di alterarlo[23]. In queste ipotesi, l'inquirente potrà agire a sorpresa ma sarà necessaria una verifica differita, in contraddittorio, circa la tecnica di riproduzione adottata unilateralmente, con conseguente inutilizzabilità nel caso in cui questa abbia irreversibilmente compromesso il dato estrapolato[24].

---

[18] «La prova informatica o elettronica (la c.d. *digital evidence*) è infatti connotata da due caratteristiche: fragilità e immaterialità. Le tracce elettroniche sono fragili in quanto facilmente alterabili, danneggiabili e distruttibili»: SENOR, *Legge 18 marzo 2008, n. 48*, cit.

[19] Ad esempio nella Circolare della Guardia di Finanza n. 1/2018 intitolata "Manuale operativo in materia di contrasto all'evasione e alla frodi fiscali", con commento di DEL CHECCO, *Le basi della* digital forensics *nella circolare 1/2018 della Guardia di Finanza*, in *ictsecuritymagazine.com*, 11 gennaio 2018, si afferma che il tradizionale "copia e incolla" non è sufficiente in quanto oltre a non permettere l'acquisizione dei *metadati*, altera anche quelli presenti sul *filesystem* se non vengono adottate precauzioni nella lettura dei dati.

[20] Secondo DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 442, «è ancora da dimostrare, in realtà, che le indagini informatiche si possano svolgere senza mutare l'oggetto su cui cadono, così come vorrebbe il legislatore».

[21] Nello stesso senso, CERQUA, *Ancora dubbi e incertezze*, cit., p. 10, MANCUSO, *L'acquisizione di contenuti* e-mail, in *Le indagini atipiche*, Torino, 2014, p. 65; CURTOTTI, *Rilievi e accertamenti tecnici*, Padova, 2013, p. 183. Secondo, FELICIONI, *Le ispezioni e le perquisizioni*, in *Trattato di procedura penale*, a cura di Ubertis, Voena, vol. XX, Milano, 2012, p. 244 s., è necessario 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».

[22] Nell'ipotesi in cui si proceda omettendo le forme e le garanzie di cui all'art. 360 c.p.p., nonostante l'assenza del requisito di urgenza, l'accertamento sarà affetto da nullità a regime intermedio *ex* artt. 178, lett. c), e 180 c.p.p., per lesione al diritto di assistenza. Così, DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, cit., p. 444.

[23] Proprio a causa della loro immaterialità, le prove digitali «permangono nella disponibilità dei potenziali responsabili anche dopo la commissione del reato: ad esempio rimangono nel *personal computer* dell'indagato, oppure sono agevolmente reperibili dal medesimo in *internet* o in altre reti informatiche, un'eventualità sempre più probabile con la diffusione del *cloud computing*»: DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, cit., p. 443.

[24] LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la* copia, in *Cass. pen.*, 2010, p. 1533, sostiene che occorra individuare soluzioni differenziate «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».

Ricostruita sommariamente la disciplina, appare nella sua evidenza la totale inadeguatezza del compendio probatorio nel caso oggetto della presente nota. Il dato informatico non è stato affatto acquisito, essendo entrato nel processo un suo surrogato: le fotografie degli SMS. Orbene, poiché sono esplicitamente dettate norme in tema di acquisizione del dato digitale, nessuna rilevanza può essere assegnata alle trascrizioni di *chat*, alle registrazioni di conversazioni o alle riproduzioni fotografiche di messaggi operate da uno degli interlocutori. L'utilizzabilità della prova documentale così entrata nel processo[25] è necessariamente condizionata dall'acquisizione del dato informatico, dovendosi necessariamente controllare «l'affidabilità della prova medesima mediante l'esame diretto del supporto onde verificare con certezza sia la paternità della registrazioni sia l'attendibilità di quanto da esse documentato»[26].

Dunque anche nel caso sottoposto alla cognizione del Tribunale di Pesaro, seguendo l'interpretazione della giurisprudenza di legittimità appena citata, la fotografia, in mancanza del dato informatico ritualmente acquisito, doveva considerarsi non utilizzabile. Tuttavia, affermare la necessarietà del dato informatico, in quanto unica prova attendibile, significa, in realtà, tacciare d'inattendibilità intrinseca la prova agli atti, in quanto priva di qualsivoglia valore dimostrativo; per tale ragione il giudizio di affidabilità degli SMS alla luce della personalità del soggetto che ne aveva la disponibilità, svolto dal Giudice, appare del tutto superfluo.

[25] Cass., sez. V, 16 gennaio 2018, n. 1822, *inedita*, chiarisce che l'acquisizione dei dati informatici dalla memoria del telefono non soggiace né alle regole stabilite per la corrispondenza, né tantomeno alla disciplina delle intercettazioni telefoniche.

[26] Cass, sez. V, 19 giugno 2017, n. 49016, N., *C.e.d. Cass.*, n. 271856.