Nuove questioni di informatica forense
ISBN 979-12-5994-643-0
DOI 10.53136/97912599464304
pp. 61-82 (gennaio 2022)

La selezione dei dati informatici in ambito giudiziario: prassi e modalità operative

Michele Ferrazzano[1], Leonardo Summa[2]

1. Introduzione

L'utilità probatoria delle informazioni memorizzate all'interno dei supporti digitali di uso quotidiano è ormai questione di informatica forense non più trascurabile per gli operatori del diritto. La rapida diffusione di dispositivi capaci di immagazzinare, con estrema facilità, una quantità considerevole di dati ed informazioni potenzialmente rilevanti nel corso di un accertamento giudiziario contribuisce ad aumentare significativamente la quantità di dati che entrano in gioco in un procedimento giudiziario allorquando un dispositivo viene raccolto.

La produzione individuale di una sempre più crescente mole di informazioni native digitali, il rapido sviluppo di soluzioni tecnologiche differenti, l'aumento della complessità delle infrastrutture tecnologiche di utilizzo quotidiano, unitamente alle caratteristiche già note del dato informatico, richiedono un elevato grado di competenze tecniche specialistiche per l'acquisizione dei dati di interesse per un determinato accertamento.

Sin dal suo ingresso, il trattamento della prova informatica nell'ordinamento giuridico italiano ha sollevato questioni di estremo interesse, pratico e scientifico, alle quali la giurisprudenza ha tentato di offrire una soluzione adeguata alla tutela delle differenti esigenze processuali. In tale solco si collocano le recenti attestazioni della Corte di Cassazione in tema di sequestro di dati informatici, testimoni di una consapevolezza più matura degli interessi in gioco e del potenziale profondamente invasivo dei mezzi istruttori a vocazione informatica nel godi-

[1] Professore a contratto di Computer forensics, Università Statale di Milano, e di Informatica, Università degli Studi di Modena e Reggio Emilia; *Digital Forensics Expert*.
[2] Cultore della materia di Informatica Giuridica e Informatica forense, Università di Bologna.

mento di diritti umani fondamentali, quali il diritto ad avere un equo processo e i corollari da esso derivati.

La spinta innovativa degli orientamenti in commento risiede nella comprensione della funzione e del reale ruolo dell'acquisizione forense di un supporto informatico negli accertamenti tecnici in ambito giudiziario, individuando la copia forense quale mezzo per la selezione, estrazione e successivo sequestro del solo materiale pertinente e rilevante con la finalità probatoria perseguita.

Nel dare attuazione agli orientamenti richiamati, l'Autorità Giudiziaria procedente deve far ricorso alle competenze specialistiche degli esperti di informatica forense e avere a disposizione gli strumenti tecnici adeguati all'esecuzione di accertamenti a carattere informatico nel rispetto delle garanzie processuali riconosciute dall'ordinamento.

In quest'ottica le modalità di selezione dei dati informatici in ambito giudiziario assumono le vesti delle nuove questioni di informatica forense, con le quali confrontarsi quotidianamente alla ricerca di un difficile punto di equilibrio tra esigenze investigative e prerogative processuali da tutelare ancora da codificare.

2. Le evoluzioni interpretative giurisprudenziali nella selezione dei dati informatici

Dal riconoscimento dell'utilità di tali strumenti informatici per la conoscenza processuale avvenuto per mano del legislatore nella l. 48/2008, la dottrina e la giurisprudenza hanno tentato di dirimere le questioni sollevate dalla crescente necessità di far ricorso all'acquisizione di elementi probatori memorizzati all'interno di supporti informatici e di offrire un tracciato da seguire nella declinazione degli strumenti investigativi a vocazione informatica[3] presente nell'impianto processuale italiano.

Nel corso evolutivo dell'interpretazione giurisprudenziale alla fenomenologia informatico-giuridica si rinvengono attestazioni di indiscusso interesse e meritevoli di approfondimento, dalla lettura delle

[3] Si fa riferimento alle interpolazioni subite dalle disposizioni del codice di procedura penale in materia di ispezioni e rilievi tecnici (art. 244, c. 2 c.p.p.), l'esame di atti, documenti e corrispondenza presso banche (art. 248, c. 2 c.p.p.), i doveri di esibizione e consegna (art. 256, c. 1 c.p.p.), gli obblighi e le modalità di custodia (art. 259, c. 2 c.p.p.), i sigilli e i vincoli delle cose sequestrate (art. 260, c. 1 e 2 c.p.p.), l'acquisizione di plichi e corrispondenza (art. 353, c. 1 e 2 c.p.p.) e, infine, gli accertamenti urgenti e il sequestro (art. 354, c. 2 c.p.p.).

quali si evince una diversa maturità di comprensione delle questioni di informatica forense, vecchie e nuove.

Si pensi agli orientamenti che hanno riconosciuto una rilevanza autonoma dell'interesse ad impugnare il sequestro della copia forense effettuata su dispositivi informatici successivamente restituiti, nei quali si valorizza – perché ben compresa – la peculiare ontologia dei dati informatici superando la tradizionale inammissibilità per sopravvenuta carenza di interesse determinata dalla restituzione del bene sottoposto a sequestro[4].

In questa direzione, per quanto di interesse nella presente trattazione, si collocano le pronunce della Cassazione che affrontano il tema della legittimità del sequestro indiscriminato di dati informatici, nelle quali viene ribadito il necessario superamento del vaglio di proporzionalità e adeguatezza della misura ablativa adottata in relazione alle esigenze probatorie, non potendosi conferire un inutile sacrificio di diritti[5].

Nello svolgimento di accertamenti a carattere informatico, in qualsiasi cornice processuale essi trovino la loro ragion d'essere, il rispetto delle migliori pratiche adoperate a livello internazionale nel trattamento della prova digitale[6] è canone ormai consolidato e riconosciuto anche dalla giurisprudenza di legittimità[7].

[4] Il richiamo è alla sentenza Cass., Sez. U., n. 40963 del 20/07/2017, Rv. 270497, che ha affermato la legittimità dell'impugnazione dell'ordinanza di conferma del sequestro probatorio di supporti informatici, restituiti previa estrazione di copia forense dei dati contenuti, qualora sia dedotto l'interesse concreto e attuale all'esclusiva disponibilità dei dati, definendo l'estensione della sussistenza del sequestro sulla copia forense estratta dal dispositivo. In tal senso, e*x multis*, le pronunce *cfr.* Cass., Sez. 5, n. 13694 del 15/02/2019, Rv. 274975; Cass., Sez. 6, n. 13306 del 22/02/2018, Rv. 272904.

[5] Sempre in tema di violazione del principio di proporzionalità e adeguatezza del sequestro probatorio di supporti informatici, nel caso specifico eseguito nei confronti di dispositivi in uso ad un giornalista, si richiama la pronuncia della Cass., Sez. 6, n. 24617/2015, che ha dichiarato l'illegittimità del sequestro indiscriminato di un sistema informatico in difetto di specifiche ragioni per l'apprensione indiscriminata dei contenuti memorizzati all'interno. Di orientamento confermativo le più recenti pronunce Cass., Sez. 6, n. 9989/2018; Cass., Sez. 6, n. 43556/2019; Cass., Sez. 6, n. 3794/2020; Cass., Sez. 6, n. 30225/2020; Cass., Sez. 6, n. 10815/2021.

[6] In particolare, si richiamano le linee guida dello Standard ISO/IEC 27037 sul trattamento della prova informatica nelle prime fasi di identificazione, raccolta e acquisizione del reperto informatico, che prescrivono la documentazione di tutte le attività eseguite, gli strumenti utilizzati e gli eventi modificativi intervenuti sul reperto al fine di garantire l'integrità e l'autenticità del contenuto acquisito con il contenuto originale disponibile. Per maggiori approfondimenti, *cfr*. *Annex* B ISO/IEC 27037 su requisiti minimi di documentazione per il trasferimento di evidenze.

[7] Ci si riferisce alla pronuncia della Cass., sez. 5, n. 49016/2017 che, qualificando i dati informatici quale prova documentale ex. 234 c.p.p., ha sancito la necessarietà dell'acquisizione forense del supporto al fine di verificare l'attendibilità e paternità del contenuto informatico riprodotto, condizionando l'utilizzabilità della trascrizione di messaggi WhatsApp all'acquisizione forense del dispositivo.

L'importanza del rispetto delle tecniche disponibili nel campo dell'informatica forense, idonee a garantire la conformità all'originale e l'inalterabilità del dato informatico acquisito, è questione di informatica forense di antico fascino e rinnovato splendore, alla luce della maggiore comprensione della realtà informatica da parte degli operatori del diritto.

Le considerazioni che derivano dall'esigenza di acquisire il dato informatico nella sua integrità sono molteplici e di trasversale interesse. In una controversia in materia di proprietà intellettuale, la tutela degli interessi della controparte (quali, ad esempio, segreti e brevetti) impone l'individuazione di criteri di analisi dei dati acquisiti che la soddisfino senza comprimere le esigenze di accertamento della parte istante.

In un accertamento tecnico in ambito penale, le considerazioni da sviluppare si moltiplicano ed investono diverse prerogative processuali. Consideriamo, ad esempio, la difficoltà di individuare i dati informatici di interesse investigativo senza ispezionarne i supporti e di bilanciare un'apprensione onnivora dei dispositivi con i vincoli di proporzionalità, adeguatezza e pertinenza imposti alle misure cautelari. Senza dimenticare come un dato informatico apparentemente non rilevante da parte di chi lo sta valutando può essere di estrema importanza per un'altra parte, sia essa già coinvolta o ancora fuori dal procedimento.

Nel tentativo di distendere una simile tensione, la giurisprudenza di legittimità ha condannato i sequestri eseguiti in maniera indiscriminata in assenza di specifiche esigenze investigative[8] che ne giustifichino l'apprensione massiva; dall'altro subordina la validità degli stessi alla difficoltà di esecuzione della selezione del solo materiale pertinente e rilevante.

La selezione del materiale pertinente è una importantissima attività che richiede agli operatori del settore un impegno significativo sotto il profilo temporale, in termini di ore-uomo e ore-macchina necessari alla selezione, ed economico, in strumenti hardware e software dedicati all'indicizzazione, ricerca e consultazione dei dati acquisiti, oltre che profonda competenza nel settore applicativo (capacità di comprendere il significato dei dati in esame) e nello specifico procedimento nel quale si opera (capacità di comprendere le pertinenza del dato in esame).

Oltre la complessità naturale delle operazioni tecniche da espletarsi nel rispetto dei principi di integrità, immodificabilità ed inalterabilità del dato acquisito deve considerarsi l'ingresso di nuovi fattori di com-

[8] Il richiamo, ancora una volta, alle pronunce citate in precedenza, specificatamente le sentenze Cass., Sez. 6, n. 43556/2019 e Cass., Sez. 6, n. 24617/2015.

plessità determinati dall'aumento delle capacità di memorizzazione, che dilatano i tempi di analisi; dalla diffusione di più dispositivi differenti per ciascun soggetto, che richiedono specifici strumenti di acquisizione; dall'evoluzione delle misure tecniche di protezione e cifratura delle informazioni, che sollecita un costante aggiornamento delle competenze necessarie.

La crescente necessità processuale del fabbisogno informativo contenuto nei supporti informatici raccomanda lo sviluppo di procedure definite e modalità operative specifiche per bilanciare le diverse esigenze contrapposte nelle singole fattispecie processuali. Nelle pagine che seguono si proporrà una possibile soluzione alle problematiche sollevate alla luce delle più recenti attestazioni della Corte di Cassazione.

3. La rivoluzione della copia-mezzo

Nel confronto quotidiano con i profili di complessità fin qui esposti, la giurisprudenza di legittimità ha offerto differenti interpretazioni della *ratio* sottesa alle novelle della l. 48/2008, nel tentativo di definire prassi e modalità operative omogenee e idonee al raggiungimento di un bilanciamento in concreto degli interessi in gioco.

In tale direzione si collocano alcune recenti attestazioni della Corte di Cassazione in tema di perquisizione e sequestro di dati informatici, che manifestano l'esigenza di procedere alla loro acquisizione nel rispetto delle *best practices* di settore e delle garanzie processuali previste, salvaguardando la tutela dei diritti fondamentali coinvolti.

Di particolare interesse è la pronuncia della Corte di Cassazione, Sez. VI Pen., n. 12904/2020, che conferma il *modus procedendi* adottato negli accertamenti informatici svolti nel caso all'esame della Corte e prefigura una modalità operativa, accolta e arricchita da successivi orientamenti, da adottare per la selezione del materiale informatico pertinente e rilevante.

> L'operazione culminata nei sequestri, secondo quanto rilevato dal Tribunale, risulta essersi svolta per gradi, dapprima essendosi individuati i dispositivi informatici e di seguito essendosi proceduto all'estrazione di copie forensi, sulla base di specifici canoni selettivi, e quanto al personal computer del ricorrente, essendosi proceduto all'estrazione di copia forense immediatamente seguita dalla fissazione, a distanza di sette giorni, della data in cui un consulente tecnico avrebbe proceduto alla selezione dei soli documenti informatici rilevanti

> sulla base delle medesime parole chiave, con immediata restituzione del resto. Si tratta di *modus procedendi* specificamente conforme a quanto in generale previsto dall'art. 247 cod. proc. pen., in funzione dell'individuazione ed estrapolazione del materiale informativo pertinente[9].

Nello specifico, il provvedimento illustra le ragioni per le quali le modalità esecutive degli accertamenti risultino conforme al dettato normativo e rendano i provvedimenti legittimi, non rilevando una violazione dei canoni di pertinenzialità, proporzionalità e adeguatezza lamentate dal ricorrente.

Come correttamente ricostruito dalla Corte, il sequestro era stato eseguito previa estrazione di copia forense da sottoporre a successiva selezione mediante criteri definiti (parole chiave, delimitazione temporale; comparazione dei digest), con restituzione del dispositivo, da effettuarsi entro un intervallo di tempo ragionevole.

Nel merito della pronuncia in commento, si confermava la proporzionalità del sequestro di materiale informatico in virtù della natura graduale della procedura adottata per l'esecuzione dello stesso.

Meritevole di approfondimento è la metodica utilizzata per l'acquisizione e la selezione degli elementi probatori di interesse: da un lato, si procedeva all'esecuzione immediata di copia forense dei dispositivi mobili sulla base di specifiche parole chiave; dall'altro, si procedeva all'acquisizione forense dell'intero contenuto di un computer con successiva nomina di un consulente tecnico incaricato per l'estrazione dei soli documenti informatici rilevanti, provvedendo alla restituzione della copia forense al termine delle operazioni.

La procedura descritta supera, a parere della Corte, il vaglio di proporzionalità richiesto per l'esecuzione della misura cautelare del sequestro e vincola l'apprensione indiscriminata del contenuto dei dispositivi informatici alla successiva selezione, realizzando un adeguato bilanciamento tra le finalità investigative e le tutele processuali previste.

Testimone del crescente fermento nella definizione di procedure adeguate al soddisfacimento delle diverse esigenze in gioco, è la pronuncia della Cassazione, Sez. VI, n. 13165/2020 che conforta la modalità operativa sin qui descritta e specifica i profili di maggior interesse nella valutazione della proporzionalità della misura adottata.

[9] *Cfr.* Corte di Cassazione, Sez. VI Pen., n. 12904/2020

> Si tratta di modalità che, riflettendo i contenuti della disciplina dettata dall'art. 247 c.p.p., comma 1 *bis*, è volta per gradi a consentire l'acquisizione di dati contenuti nel sistema informatico e nel contempo ad assicurare la minor invasività dell'operazione a vantaggio della parte interessata: ciò che occorre è tuttavia il rispetto dei menzionati profili qualitativi, quantitativi e temporali. […] Ma se di per sé è garantita la continuità operativa e sono definiti i limiti della ricerca, non può parlarsi di un'invasività non giustificata[10].

Nella fattispecie all'attenzione della Corte, veniva esaminata la legittimità dell'ordinanza del Tribunale che disponeva la distruzione delle copie forensi acquisite e dei dati non pertinenti al *thema probandum*, cogliendo l'occasione per approfondire la proporzionalità della misura adottata e definire i limiti operativi nell'acquisizione di materiale informatico.

La massima espressa dalla pronuncia in commento riconosce come il bilanciamento tra le finalità investigative e le esigenze di tutela coinvolte nell'accertamento richieda un'adeguata valutazione sotto il profilo quantitativo, qualitativo e temporale della proporzionalità della misura adottata.

In altri termini, sotto il profilo quantitativo occorre verificare la sussistenza del nesso di pertinenzialità tra il supporto informatico oggetto di accertamento e il *thema probandum*, specificando l'idoneità probatoria dei dati contenuti e oggetto di interesse investigativo; sotto il profilo qualitativo, invece, è necessario valutare la strumentalità dell'apprensione integrale, mediante copia forense, all'individuazione garantita dei dati rilevanti e pertinenti; infine, sotto il profilo temporale bisogna contemperare la necessità di procedere ad operazioni tecniche in differita con l'interesse a rientrare in possesso dei beni oggetto di accertamento.

Sintetizzando le argomentazioni della Corte, in tema di acquisizione di elementi probatori informatici, la legittimità dell'estrazione mediante copia forense del contenuto integrale di un dispositivo informatico deve essere valutata «sotto il profilo ontologico in rapporto alla fase in cui si inserisce, in funzione della separata estrazione dei soli dati realmente rilevanti»[11], non potendo sindacare un'invasività non giustificata di tale

[10] *Cfr.* Corte di Cassazione, sez. VI penale, sentenza 28 aprile 2020 (ud. 4 marzo 2020), n. 13165/2020

[11] *Cfr.* Corte di Cassazione, sez. VI penale, sentenza 28 aprile 2020 (ud. 4 marzo 2020), n. 13165/2020

acquisizione «se di per sé è garantita la continuità operativa e sono definiti i limiti della ricerca»[12].

Perciò, al termine della selezione ed estrazione dei dati rilevanti, la copia forense acquisita non può che essere restituita all'avente diritto, in luogo della distruzione disposta dal Tribunale, quale forma di reintegro al possesso esclusivo dei dati contenuti nella copia forense.

Il rapporto tra l'utilità processuale delle informazioni contenute nei dispositivi informatici e il cambiamento imposto ai tradizionali modelli investigativi è efficacemente rappresentato nella sentenza della Corte di Cassazione, sez. VI, n. 34265/2020[13].

In prima battuta, la pronuncia in commento ricostruisce i limiti della legittimità del sequestro probatorio segnati dalla verifica, caso per caso, del nesso di pertinenzialità e strumentalità tra la *res* – dispositivo informatico – i fatti contestati e la finalità probatoria da soddisfare. In sede di verifica, quindi, occorrerà valutare la proporzionalità e la ragionevolezza della motivazione posta a fondamento della misura adottata e della sussistenza del nesso di strumentalità funzionale all'accertamento dei fatti[14].

Ciò è vero, a maggior ragione, nel contesto degli accertamenti informatici in cui vi è, da un lato, l'interesse investigativo all'acquisizione dei dati rilevanti nel rispetto delle misure tecniche a garanzia dell'integrità e inalterabilità di quanto acquisito, che richiedono competenze specialistiche di difficile attuazione negli atti a sorpresa; dall'altro, l'esigenza di tutela dei diritti fondamentali del soggetto sottoposto alla misura, evitando un inutile sacrificio dei diritti limitati dalla misura[15].

Addentrandosi nell'esame delle misure tecniche atte a garantire l'acquisizione genuina del dato informatico, caratterizzata dall'inalterabilità e dalla conformità all'originale del contenuto acquisito, la Corte offre una lucida interpretazione del portato normativo introdotto dalle interpolazioni della l. 48/2008 al codice di rito.

[12] *Cfr*. Corte di Cassazione, sez. VI penale, n. 13165/2020, cit.

[13] *Cfr*. Corte di Cassazione, sez. VI penale, sentenza 22 settembre 2020 (dep. 2 dicembre 2020), n. 34265

[14] Si ribadisce l'importanza dell'onere motivazionale in ordine al nesso di strumentalità tra la res informatica rispetto all'accertamento penale e della sua necessaria esplicitazione nel decreto di sequestro, in quanto funzionale a garantire che la misura adottata non arrechi un inutile sacrificio di diritti, il cui esercizio di fatto non pregiudicherebbe la finalità probatoria/cautelare perseguita, richiamando le pronunce SS.UU. n. 36072/2018 e la più nota pronuncia della Corte Cost. n. 85 del 2013.

[15] Per approfondimenti si veda il contributo di L. Bartoli, *Parità delle armi e e-discovery nel processo penale: quali indicazioni da Strasburgo?*

Infatti, richiamati i riferimenti alle varie modalità di acquisizione di dati informatici previsti dal codice di procedura[16], chiarisce come la creazione della copia forense di un dispositivo informatico sia la *procedura più adeguata a garantire l'integrità dei dati*, che richiede, nella prassi quotidiana, il sequestro del dispositivo per l'acquisizione e successiva selezione dei dati pertinenti alle finalità probatorie perseguite.

La portata innovativa della pronuncia in commento risiede nella corretta collocazione, sul piano tecnico-giuridico, del nucleo informativo acquisito mediante la creazione della copia forense che vale la pena di riportare nella sua interezza:

> Non rileva in sé come cosa pertinente al reato in quanto essa contiene un insieme di dati indistinti e magmatici rispetto ai quali nessuna funzione selettiva è stata compiuta al fine di verificare il nesso di strumentalità tra res, reato ed esigenza probatoria. Ne deriva, come è stato specificato dalla Corte di cassazione, che la c.d. copia integrale costituisce solo una copia-mezzo, cioè una copia che consente di restituire il contenitore, ma che non legittima affatto il trattenimento dell'insieme di dati appresi (Sez. 6., n. 13165 del 04/03/2020, Scagliarini). La copia integrale consente di fare, dopo il sequestro, ciò che naturalmente avrebbe dovuto essere fatto prima, cioè la verifica di quali, tra i dati contenuti nel contenitore, siano quelli pertinenti rispetto al reato. La c.d. copia integrale è una copia servente, una copia mezzo, e non una copia fine[17].

Il riconoscimento del carattere servente della copia forense produce un duplice effetto: vincola il trattenimento della copia forense esclusivamente per una cornice temporale definita e strettamente necessaria alla selezione delle sole informazioni conferenti con la funzione probatoria sottesa al sequestro; al termine della selezione degli elementi pertinenti al *thema probandum* si dovrà provvedere alla restituzione della copia integrale agli aventi diritto, non potendosi disporre il sequestro probatorio di res non necessarie per l'accertamento dei fatti.

In conclusione, la Corte definisce i limiti del provvedimento di sequestro probatorio informatico, rilevando che:

[16] Nello specifico le prescrizioni atte a garantire l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, contenute negli articoli in materia di ispezioni (art. 244, c. 2, c.p.p.), perquisizioni (art. 247, c. 1 *bis*, c.p.p.) e sequestro di dati informatici presso fornitori di servizi (art. 254 *bis* c.p.p.), come anche in materia di accertamenti urgenti da parte della polizia giudiziaria (art. 354, c. 2, c.p.p.).

[17] *Cfr*. Cass. pen., Sez. VI, 22 settembre 2020 (dep. 2 dicembre 2020), n. 34265

> Il Pubblico Ministero: a) non può trattenere la c.d. copia integrale dei dati appresi se non per il tempo strettamente necessario alla loro selezione; b) è tenuto a predisporre una adeguata organizzazione per compiere la selezione in questione nel tempo più breve possibile, soprattutto nel caso in cui i dati siano stati sequestrati a persone estranee al reato per cui si procede; c) compiute le operazioni di selezione, la c.d. copia - integrale deve essere restituita agli aventi diritto[18].

La portata innovativa della pronuncia in commento si distingue chiaramente nella definizione di una procedura operativa, descritta nell'elenco richiamato, che realizza lucidamente il difficile bilanciamento dell'interesse investigativo dei dati informatici e le esigenze di tutela processuale della proporzionalità delle misure.

In tema di apprensione di dati informatici, meritevole di approfondimento è la Sentenza della Cassazione penale, sez. II, del 23/09/2020, n. 37941 per la efficace ricostruzione degli orientamenti giurisprudenziali in materia e per le motivazioni esposte a sostegno dell'adesione all'orientamento mediano tra quelli presentati[19].

Nella vicenda in esame, da un lato, veniva eseguito il sequestro probatorio di dispositivi informatici, per i quali si disponeva di procedersi ad accertamento tecnico non ripetibile (art. 360 c.p.p.) per la formazione della copia forense; dall'altro si procedeva al sequestro della sola copia forense e della posta elettronica, per i quali si disponeva un accertamento tecnico finalizzato all'estrazione del materiale rilevante a breve distanza dal sequestro.

I ricorsi esaminati dalla Corte deducevano la violazione di legge in ordine alla mancata identificazione delle finalità probatorie del vincolo imposto e al difetto di proporzionalità del materiale sottoposto a sequestro, acquisito senza eseguire alcuna attività perquirente diretta alla selezione dei dati di interesse da sottoporre a successivo sequestro.

La decisione di rigetto viene motivata sulla scorta di un iter argomentativo di fascinosa linearità che, ricostruendo le attestazioni giurisprudenziali in tema di acquisizione di dati informatici[20], afferma la

[18] *Cfr*. Cass. pen., Sez. VI, sent. n. 34265/2020, cit.

[19] *Cfr*. Cass. pen., Sez. II, 23 settembre 2020 (dep. 31 dicembre 2020), n. 37941.

[20] La pronuncia in commento ricostruisce gli orientamenti in materia di sequestro di dati informatici. Nello specifico richiama: a) le sentenze che hanno affermato la legittimità del sequestro dell'intero supporto informatico piuttosto che l'estrazione dei singoli dati quando la misura sia giustificata dalle difficoltà tecniche di estrapolare con riproduzione mirata i dati contenuti nella memoria informatico (Sez. V, n. 38456 del 17/05/2019 - dep. 17/09/2019, Benigni, Rv. 277343; Sez. V, n. 16622 del 14/03/2017 - dep. 04/04/2017, Storari, Rv. 270018);

funzionalizzazione del sequestro imposto all'intero supporto ad una analisi tecnica diretta all'individuazione dei dati rilevanti per la prosecuzione delle indagini.

Nello specifico, chiarita la funzione proattiva e l'onere motivazionale del sequestro probatorio delle cose pertinenti al reato, la Corte si sofferma nella declinazione dei principi generali, da tempo affermati nella giurisprudenza[21], all'apprensione dei dati contenuti in supporti informatici in quanto, pur non costituendo il corpo del reato, si rendono necessari all'accertamento dei fatti delineati nella notizia di reato.

Secondo l'orientamento della Corte, nella valutazione della proporzionalità del sequestro di dati informatici in qualità di cosa pertinente al reato occorre verificare la sussistenza e la corretta individuazione nel provvedimento genetico dei seguenti elementi:

> (a) deve essere identificato il fumus del reato per cui si procede ed il collegamento tra tale reato e i dati informatici che si intendono vincolare individuando così il nesso di "pertinenza"; (b) deve essere indicata la finalità probatoria che sorregge il vincolo; (c) se non si vincolano i dati, ma l'intero supporto (o tutti

b) le pronunce che hanno dichiarato l'illegittimità, per violazione del principio di proporzionalità e adeguatezza, del sequestro informatico a fini probatori che conduca in assenza di specifiche ragione ad un'indiscriminata apprensione di tutte le informazioni contenute. Tale orientamento ha trovato principale applicazione in fattispecie riguardanti dispositivi sequestrati a giornalisti (Sez. VI, n. 24617 del 24/02/2015 - dep. 10/06/2015, Rizzo, Rv. 264092; Sez. VI, n. 9989 del 19/01/2018 - dep. 05/03/2018, Lillo e altri, Rv. 272538) ma anche in situazioni diverse avente ad oggetto il sequestro dell'intero archivio cartaceo di un'azienda senza indicazione specifica dei documenti funzionali all'accertamento dei fatti (Sez. VI, n. 43556 del 26/09/2019 - dep. 24/10/2019, Scarsini, Rv. 277211); c) l'orientamento mediano che ritiene legittimo il sequestro informatico dai contenuti estesi, perché dati potenzialmente rilevanti per le indagini, purché si provveda, nel rispetto del principio di proporzionalità e adeguatezza, alla immediata restituzione delle cose sottoposte a vincolo, non appena sia decorso il tempo ragionevolmente necessario per gli accertamenti (Sez. VI, n. 53168 del 11/11/2016 - dep. 15/12/2016, Amores, Rv. 268489). Il collegio nel dare continuità all'orientamento mediano, precisa come il sequestro non debba essere necessariamente preceduto dalla perquisizione informatica, che necessita la predisposizione di competenze specialistiche incompatibili con l'effetto a sorpresa della perquisizione stessa. In conclusione, la pronuncia in commento valorizza, nella valutazione di proporzionalità del sequestro di supporti informatici, la variabile "tempo" necessaria per l'estrazione dei dati rilevanti.

[21] Richiamando testualmente l'ultimo capoverso del punto 1.1 del considerato in diritto della pronuncia in commento «il sequestro può ritenersi meramente "esplorativo" e, dunque illegittimo solo quando non si sia in presenza di una notizia di reato sufficientemente delineata e suscettibile di approfondimenti istruttori che legittima il sequestro a fini investigativi delle cose pertinenti al reato» (Sez. 6, n. 3187 del 07/01/2015 - dep. 22/01/2015, Boselli, Rv. 262084; Sez. 3, n. 24561 del 17/05/2012 - dep. 20/06/2012, Vicentini e altro, Rv. 252767).

> i dati in modo indistinto) deve essere, altresì, identificata la ragione della necessità del sequestro "integrale", di regola riconducibile alla impossibilità di effettuare la selezione tecnica preventiva, che richiede la predisposizione di una attività tecnica e competenze specialistiche[22].

Dunque, la legittimità del vincolo imposto ad una massa indistinta di dati potenzialmente rilevante per l'attività investigativa deve essere riconosciuta ogni qualvolta risulti funzionale all'esecuzione di accertamenti tecnici diretti all'identificazione degli elementi utili alla prosecuzione delle indagini e, perciò, sia limitato al tempo strettamente necessario all'esecuzione delle operazioni di acquisizione e selezione dei dati di interesse.

Il solco tracciato dalle sentenze in commento è avamposto alla codificazione di prassi e modalità operative ampiamente in uso nella pratica quotidiana degli accertamenti a carattere informatico, meritevole di trovare adeguato riconoscimento nel codice di rito tramite l'introduzione di una procedura autonoma per la selezione di dati informatici.

Dunque, da un lato viene garantita la legittimità di sequestri indiscriminati di materiale informatico, vincolata temporalmente all'esecuzione delle operazioni tecniche necessarie per l'accertamento richiesto, dall'altra viene sindacata la proporzionalità del provvedimento emesso dall'Autorità Giudiziaria in mancanza di criteri specifici da adottare nella selezione del solo materiale pertinente e rilevante per l'accertamento in parola, da sottoporre a successivo sequestro mediante la formazione di una copia forense del solo materiale selezionato.

La procedura descritta consente di limitare, da un lato, l'invasività del sequestro del dispositivo, provvedendo in tempi brevi all'acquisizione forense integrale e alla restituzione del supporto acquisito; dall'altro permette di circoscrivere il carattere esplorativo della misura eseguita all'acquisizione del solo materiale derivato dalla selezione dei contenuti secondo criteri predefiniti e calibrati sulle esigenze investigative della singola fattispecie.

Tuttavia, nell'adozione di una simile procedura operativa vi sono profili critici meritevoli di essere adeguatamente attenzionati e valutati nella cornice processuale di riferimento. In particolare, in ambito penale il rischio concreto che si profila è quello di aggirare i tradizionali principi processuali che sostengono l'impianto accusatorio del processo penale, lasciando nella piena disponibilità degli organi inquirenti tutto

[22] *Cfr*. Cass. pen., Sez. II, n. 37941/2020, cit.

il materiale acquisito e non ancora vagliato. O, peggio, mettere dati riservati a disposizione di terzi comunque coinvolti nel procedimento, con il rischio di divulgazione di informazioni riservate o sulla vita privata che nulla hanno a che vedere con i procedimenti giudiziari nei quali sono stati raccolti[23].

4. Le modalità operative adottate nella selezione di dati informatici in ambito giudiziario

In qualsiasi ambito di accertamento divenga necessario acquisire le informazioni contenute nei dispositivi di uso quotidiano, occorre far riferimento alle indicazioni fornite dagli standard di settore, spesso condensati nel termine *best practices*[24]. Nel campo dell'informatica forense, le linee guide da adottare nel trattamento della prova digitale sono codificate nello standard internazionale ISO/IEC 27037, che indica i principi e le procedure da rispettare nelle specifiche attività di identificazione, raccolta, acquisizione, conservazione e trasporto di una fonte di prova digitale. Ad esso, si aggiungono le differenti procedure operative pubblicate da organizzazioni internazionali, europei e nazionali[25], nel tentativo di definire modelli operativi applicabili in maniera omogenea alle differenti situazioni in cui risulta necessario assicurare l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Come noto, la definizione di simili procedure e *best practice* nello svolgimento degli accertamenti informatici ha l'obiettivo di garantire

[23] Sul carattere onnivoro degli accertamenti informatici eseguiti senza alcuna previa selezione o indicazione dei criteri selettivi da adottare si veda la recente sentenza Cass. pen., Sez. VI, 28 settembre 2021 (dep. 27 ottobre 2021), n. 38460. Di sicuro interesse è l'esplicitazione dei corollari necessari alla dichiarata illegittimità del provvedimento di sequestro, che comporta l'estensione dell'illegittimità della massa di dati acquisita e la restituzione all'avente diritto di tutte le copie forensi illegittimamente acquisite.

[24] Per una disamina più ampia dello stato attuale delle best practices, si veda R. BRIGHI, M. FERRAZZANO, *Digital forensics: best practices and perspective*, in Caianiello M., Camon A. (a cura di), *Digital forensics evidence. Towards common european standards in antifraud administrative and criminal investigations*, Wolters Kluwer, 2021, pp. 13-48.

[25] Oltre agli standard internazionali, di particolare interesse sono le best practice di settore pubblicate dalle diverse organizzazioni, come American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST), Scientific Working Group on Digital Evidence (SWGDE), IOCE (International Organization of Computer Evidence), IACIS (International Association of Computer Investigative Specialist), ACPO (Association of Chief Police Officer).

l'acquisizione di dati in forme tali da assicurarne l'integrità, l'autenticità e l'inalterabilità di quanto acquisito e soddisfare le esigenze di verificabilità delle operazioni eseguite, cercando di uniformare il modo di procedere degli operatori tecnici coinvolti – la cui formazione specifica in materia e quindi competenza tecnica è spesso variegata – che altrimenti potrebbero dare eccessivo sfogo alla propria fantasia (come peraltro comunque capita non essendo tali standard vincolanti).

A tale scopo è opportuno predisporre di un'adeguata conoscenza dei processi e dei requisiti richiesti per assicurare una concreta applicazione dei principi esplicitati dalle linee guida riconosciute a livello internazionale. Di interesse primario sarà individuare le competenze tecniche necessarie all'esecuzione delle attività sui reperti informatici, per il tramite di figure professionali in possesso di adeguate competenze tecniche[26] in grado di garantire la raccolta di tutti gli elementi informatici utili nel rispetto dei requisiti di verificabilità, affidabilità e giustificabilità delle operazioni svolte[27].

La fragilità del dato informatico, per le sue congenite caratteristiche effimere, impone di considerare con particolare attenzione le fasi dell'acquisizione e della conservazione della prova digitale, maggiormente suscettibili di comprometterne l'integrità e l'autenticità del dato informatico acquisito[28].

Un aspetto doveroso da chiarire riguarda la motivazione per la quale si esegue copia forense dei dati informatici: in informatica forense, a differenza di altre scienze forensi, è possibile duplicare in quantità infinita i dati che devono essere sottoposti ad analisi. Tale circostanza gioca a favore tanto di questioni di carattere logistico, permettendo di

[26] *Cfr*. *Annex* A ISO/IEC 27037.

[27] Nello specifico, per affidabilità si intende che tutti i processi eseguiti devono essere ben documentati producendo un risultato ripetibile utilizzando, in qualsiasi momento, la stessa procedura e metodo di misurazione, stessi strumenti e nelle stesse condizioni; la verificabilità delle operazioni richiede di garantire, documentando tutte le attività svolte, ad un consulente tecnico informatico terzo la facoltà di verificare le attività svolte, valutando metodo scientifico, le tecniche e le procedure seguite; infine per giustificabilità si richiede di essere in grado di dimostrare che le scelte adoperate erano le migliori possibili o le uniche possibili per ottenere tutte le potenziali prove digitali.

[28] Per una disamina esaustiva della necessità di acquisire correttamente il dato informatico, si veda C. MAIOLI, *Dar voce alle prove: elementi di informatica forense*, in Pozzi P., Masotti R. e Bozzetti M. (a cura di), Crimine virtuale, minaccia reale, a cura di FrancoAngeli, 2004. Sull'importanza della corretta metodologia da adottare nel trattamento della prova informatica, dalla sua acquisizione alla successiva analisi, si veda S. ATERNO, P. MAZZOTTA, *La perizia e la consulenza tecnica – con approfondimento in tema di Perizie Informatiche (analisi e schede tecniche di D. Caccavella)*, CEDAM, 2006.

distribuire il lavoro tra più analisi o di parallelizzare e rendere autonome le parti coinvolte, quanto di poter differire nel tempo e geograficamente l'analisi rispetto al luogo e all'epoca in cui ci si approccia al dato per la prima volta.

La creazione di copia forense ha, dunque, come fine primario quello di preservare il dato e spostarlo nel tempo e nello spazio, senza che tale operazione possa cagionare alcuna perdita di informazioni.

Tuttavia, da un punto di vista normativo, non risulta alcun ordinamento giuridico che imponga l'acquisizione totale, ossia bit a bit, di dati informatici, bensì vi è un generico richiamo all'adozione di soluzioni atte a garantire integrità e attendibilità dei dati informatici da utilizzare come prova.

Ne consegue che deve essere "scardinata" questa idea per la quale la prova informatica è la copia forense bit a bit, essendo in realtà tale operazione tecnica semplicemente a servizio della fase di analisi dei dati ivi contenuti. Per sostenere la tesi per la quale non è solo la copia bit a bit a doversi considerare "copia forense" è sufficiente spostarsi dal primigenio ambito della *disk forensics* "pura" e prendere in considerazione tutto l'ambito della *mobile forensics*. In tale branca è piuttosto raro che si esegua una copia bit a bit, sia per ragioni tecniche di impossibilità o estrema difficoltà, sia per non intellegibilità dei dati, spesso cifrati, preferendo una soluzione di acquisizione di altro tipo (backup, file system o addirittura fotografica). Si pensi, inoltre, pur rimanendo nel contesto di disk forensics, a tutti quei casi in cui è più che sufficiente acquisire un sottoinsieme di dati, per i quali il dato informatico oggetto di accertamento prescinde dal contesto nel quale è memorizzato (ad esempio, in un caso di contenzioso su un codice sorgente appare superflua l'acquisizione di tutto il sistema informatico che lo contiene).

Chiarito, dunque, quale sia il vero ruolo di una copia forense in un accertamento tecnico di informatica forense, a prescindere dalla modalità e dall'estensione della stessa, si approfondisce nel seguito la modalità di analisi per selezionare i soli dati informatici rilevanti per il procedimento.

5. L'e-discovery per la selezione del materiale rilevante

Dopo aver assicurato una corretta acquisizione e conservazione del reperto informatico, occorre definire i limiti e gli obiettivi dell'analisi fo-

rense da svolgersi sui reperti acquisiti e valutare le risultanze dell'investigazione condotta, presentando gli esiti ottenuti e motivando il percorso scientifico a fondamento delle valutazioni svolte in sede di analisi.

Sebbene tale operazione presenti profili di rischio piuttosto bassi, svolgendosi su una copia terza (c.d. copia lavoro), resiste comunque la necessità di adeguate competenze tecniche per la corretta interpretazione e valutazione delle evidenze informatiche ottenute.

A supporto degli operatori di settore, vi sono procedure consolidate per la conduzione dell'analisi e la ricerca di evidenze memorizzate in formato elettronica, condivise a livello internazionale e recepite nello standard ISO/IEC 27050 che identifica i criteri e i requisiti del c.d. processo di e-discovery.

L'*electronic discovery* è il processo che, nell'ambito delle attività di informatica forense, consente di ricercare e individuare informazioni pertinenti e rilevanti memorizzate in formato digitale (in inglese *electronically stored information*, abbreviato in ESI). Lo standard citato definisce le differenti tipologie e sorgenti di ESI, le molteplici modalità di rappresentazione delle informazioni individuate e le fasi in cui si articola il processo, sovrapponibili a quelle previste per il trattamento della prova digitale[29].

Ogni informazione digitale potenzialmente rilevante deve essere individuata all'interno di una crescente quantità di dati provenienti da fonti molteplici e di uso promiscuo, che dovranno essere acquisite e conservate preservando l'integrità del dato da interventi modificativi e,

[29] Le tipologie descritte dallo standard sono definite dalla distinzione tra dati immediatamente accessibili (*active data*) e dati non immediatamente accessibili (*inactive, residual, legacy data*). Nella tipologia dei c.d. *active data* rientrano tutti i dati memorizzati all'interno del supporto e visibili all'utente nel normale utilizzo del dispositivo; in quella dei *c.d. inactive data* rientrano tutti i dati archiviati e non disponibili all'utente, memorizzati in automatico dai sistemi di backup, spesso custoditi presso fornitori terzi; nella categoria dei c.d. *residual data* vi sono i file nascosti utilizzati dal sistema operativo in uso, quelli danneggiati o cancellati; infine, all'interno dei c.d. *legacy data* rientrano tutte le informazioni generate da sistemi informatici per i quali il produttore non rilascia più aggiornamenti. Le diverse tipologie di fonti sorgenti di ESI sono divise nelle c.d. *Custodian data sources*, ovvero supporti sui quali un determinato utente ha il diretto controllo o gestione, e nelle c.d. *Non-custodian data sources*, ovverosia infrastrutture per la gestione di più informazioni sotto il controllo di un amministratore, come NAS, database e applicazioni per la condivisione di ESI, cloud storage. Infine, tra e forme di rappresentazione per la produzione delle ESI, lo standard prevede la seguente classificazione dei formati: a) *native* e b) *near-native,* consigliata per file non progettati per la stampa come database, fogli di calcolo, etc.; c) *image (near- paper)* e d) *paper*, per la produzione di immagini visive o dati progettati per essere stampati su carta.

successivamente elaborate, mediante il processo di indicizzazione dei contenuti acquisiti, per essere ricercabili mediante criteri predefiniti, calibrati sulle esigenze investigative del caso.

Nella selezione di informazioni potenzialmente rilevanti, le tecniche di ricerca automatizzate a supporto degli operatori del settore sono molteplici e diversamente utili a seconda del contesto investigativo. Nella ricerca di contenuti difficilmente modificabili, l'individuazione dei contenuti di interesse può essere agevolmente effettuata mediante la comparazione delle impronte hash contenute in un insieme di digest noto con quelle dei dati acquisiti[30].

Di maggior diffusione è la metodologia della ricerca per parola chiave, che consente di individuare i dati di interesse utilizzando stringhe di ricerca, composte da termini specifici, diversamente declinabili a seconda della loro utilità. Il rischio di selezionare ed esaminare una grande quantità di falsi positivi è strettamente correlato al grado di specificità dei termini impiegati e alla granularità dei criteri di ricerca utilizzati.

In tale contesto, occorre dedicare particolare attenzione all'individuazione degli obiettivi dell'accertamento e alla definizione di stringhe di ricerca specifiche, combinate con ulteriori condizioni di validità dei riscontri ottenuti, utili all'isolamento del solo materiale di interesse da sottoporre alla successiva valutazione degli attori coinvolti nell'accertamento.

Le differenti tipologie di ricerche per parola chiave permettono di costruire stringhe di ricerca calibrate sulle peculiari esigenze investigative del caso, ricorrendo alla ricerca di termini per corrispondenza esatta, per corrispondenza approssimativa, vincolati alla validità di operatori booleani o di differenti logiche adottate[31].

Pertanto, la selezione di dati di interesse nell'ambito di un accertamento giudiziario dovrà essere attentamente progettata, identificando i parametri da attribuire all'indicizzazione dei contenuti acquisiti e definendo il perimetro della ricerca e dei criteri da applicare nella selezione

[30] Ad esempio, nelle indagini per reati pedopornografici l'utilizzo di un archivio di immagini e video già noti e segnalati per essere contenuti pedopornografici, l'analisi dei dati acquisiti può essere agevolmente comparando le impronte hash dei dati acquisiti con quelli già noti. La stessa logica viene utilizzata negli accertamenti per violazioni in materia di diritto d'autore, proprietà intellettuale.

[31] Ad esempio, gli algoritmi di ricerca che adottano la logica *fuzzy*, evoluzione della logica booleana che consente di attribuire validità logica diverse da vero e falso; oppure la logica *stemming*, per individuare parole derivate dal termine utilizzato; o, ancora, una ricerca per fonemi che permette di individuare parole con stessi fonemi.

del materiale, permettendo di ampliare e restringere la pertinenza dei riscontri ottenuti.

Si noti che tali modalità sono ampiamente in uso nei procedimenti civili relativi a violazioni di segreti industriali, allorquando a seguito di una raccolta dati anche massiva in sede di descrizione, il Giudice solitamente nomina un proprio Consulente Tecnico d'Ufficio affinché possa selezionare unicamente il materiale pertinente con l'oggetto del ricorso o dell'atto di citazione, applicando questo genere di filtri per isolare il solo insieme di file di rilievo e non consentendo alla parte ricorrente di disporre di tutti gli altri dati.

La stessa modalità di selezione di dati rilevanti con tecniche di e-discovery è ampiamente utilizzata in ambito difensivo da parte anche di studi legali che, attraverso idonee piattaforme di e-discovery, permettono la collaborazione parallela da parte di più utenti nel vaglio della documentazione disponibile, sia essa acquisita dal fascicolo processuale o nell'ambito di proprie indagini difensive. Tali piattaforme consentono, tra le altre, di classificare i dati tramite etichette che permettono, attraverso raffinamenti successivi, di potersi focalizzare sulle sole informazioni rilevanti.

6. Protocolli in uso

La necessità di selezionare il solo materiale di interesse investigativo, all'interno della massa magmatica delle informazioni memorizzate in supporti digitali, si manifesta con evidenza nella prassi quotidiana delle investigazioni informatiche, in qualsiasi cornice processuale.

Ad esempio, negli accertamenti in materia di proprietà intellettuale, in cui spesso le informazioni di interesse sono esclusivamente disponibili in formato digitale, si rende necessario procedere ad un'attenta selezione ed estrazione dei soli dati rilevanti per i fatti oggetto di accertamento, contemperando le esigenze di riservatezza delle informazioni acquisite.

Nell'esecuzione di provvedimenti di descrizione, ex art. 129 c.p.i., lo svolgimento della fase cautelare di raccolta degli elementi utili all'accertamento è prassi quotidiana ricorrere ai principi e alle linee guida contenuti negli standard richiamati. Di fatti, in esecuzione del decreto si provvede al congelamento dei dati potenzialmente rilevanti mediante acquisizione forense della memoria dei supporti descritti; suc-

cessivamente si procede ad un'analisi sommaria, per la tipologia di procedura, dei possibili riscontri ottenuti dalle ricerche effettuate per confermare o smentire gli elementi probatori a sostegno del ricorso presentato.

Allo stesso modo, ciò si rende necessario nell'ambito delle indagini aziendali nei casi in cui occorre raccogliere, esaminare e documentare il riscontro di evidenze informatiche, contenute nei supporti informatici aziendali, a dimostrazione di condotte giuridicamente rilevanti. Sebbene sia in una fase prodromica all'instaurazione di un procedimento giudiziario, risulta altrettanto importante eseguire gli accertamenti informatici nel rispetto delle *best practices* di settore, sia in termini di validità probatoria degli elementi informatici raccolti e in termini di efficacia dell'azione legale proposta.

E, come si è visto, ciò risulta a maggior ragione utile negli accertamenti in ambito penale in cui occorre bilanciare, nello svolgimento delle attività tecniche, le diverse prerogative e tutele processuali in gioco. L'esigenza investigativa di eseguire provvedimenti preservando il carattere "a sorpresa" dei mezzi istruttori tradizionali deve misurarsi con la necessità di avere a disposizione competenze tecniche specialistiche in grado di assicurare l'acquisizione dei dati in conformità con le prescrizioni del codice di rito poste a garanzia dell'esercizio del diritto di difesa.

Spesso, tale difficoltà operativa impone, solo per i dispositivi fisicamente disponibili sul luogo di intervento, di procedere all'apprensione del supporto contenente informazioni di interesse investigativo, sottoponendolo alla misura del sequestro probatorio, prodromica all'esecuzione di accertamenti tecnici finalizzati all'acquisizione forense dei contenuti e alla successiva selezione ed estrazione dei dati informatici rilevanti. Permangono in ogni caso le esigenze di acquisire nell'immediatezza delle attività i dati di sistemi che non possono essere oggetto di ablazione per esigenza di continuità del servizio (si pensi, ad esempio, a un server di un ospedale) o per impossibilità di apprensione della *res* (dati memorizzati in sistemi remoti e disponibili in *cloud*).

Le prerogative processuali in ambito penale richiedono di costruire procedure e modelli operativi in cui poter trovare, a seconda della fattispecie, il giusto bilanciamento degli interessi coinvolti nell'accertamento, garantendo l'esecuzione delle operazioni tecniche nel rispetto delle best practices di settore e la partecipazione dei soggetti coinvolti per l'esercizio dei propri diritti.

7. Prospettive *de iure condendo*

Come abbiamo visto nelle recenti attestazioni giurisprudenziali, la crescente importanza probatoria dei dati informatici, memorizzati nei diversi dispositivi di uso quotidiano, ha plasmato l'interpretazione delle novelle introdotte dalla l. 48/2008 negli accertamenti a vocazione informatica. Maggior importanza viene data alla successiva fase di selezione ed estrazione del materiale di interesse, vincolando la legittimità del provvedimento alla definizione di criteri chiari e specifici per la ricerca e selezione all'interno della copia forense acquisita.

Dalla lettura delle evoluzioni interpretative fin qui commentate, si delinea una procedura operativa in cui l'iter da seguire è il seguente:

1. apprensione del supporto contenente dati di interesse, specificando il nesso di pertinenzialità, la finalità probatoria e la ragione del sequestro integrale del supporto con i dati informatici di interesse;
2. definizione di criteri per la selezione dei dati rilevanti rispetto al provvedimento di sequestro e successiva elaborazione dei contenuti mediante *tool* di indicizzazione e ricerca (per parola chiave, per hash, per periodo temporale, per adiacenza di percorso di salvataggio, per esame visivo manuale, ecc.) dei contenuti acquisiti;
3. formazione di una copia forense, da intendersi come insieme di dati selezionati e relativi hash, contenente i soli dati pertinenti e rilevanti oggetto di selezione, con restituzione della copia integrale all'utilizzatore del dispositivo.

L'adozione della procedura appena descritta è già da tempo in uso nella prassi degli operatori del settore nelle investigazioni difensive, mentre lo è raramente in quelle dell'Autorità Giudiziaria, trovando applicazione solo nei rari casi in cui i consulenti tecnici coinvolti sono in possesso di specifiche competenze tecniche e giuridiche oltre che di carisma per poter sostenere la validità tecnico-giuridica di tali procedure di fronte al dibattito processuale. Ciò in quanto tale procedura non è espressamente codificata all'interno del codice di rito ed è soggetta alla discrezionale applicazione dell'Autorità Giudiziaria procedente. Una simile lacuna legislativa presenta molteplici profili di rischio meritevoli di approfondimento e che richiedono di immaginare

nuove vesti processuali agli accertamenti giudiziari a vocazione informatica[32].

Sotto il profilo investigativo occorre, da un lato, assicurare l'efficacia del carattere a sorpresa che connota i mezzi di ricerca della prova, senza che ciò subisca limitazioni in virtù della complessità tecnica delle operazioni da eseguire; dall'altro, occorre prevenire le derive esplorative derivanti dall'acquisizione effettuata senza previa verifica della pertinenza dei contenuti memorizzati all'interno del supporto sequestrato.

Dalla prospettiva difensiva delle indagini penali a vocazione informatica, è di primaria importanza definire modalità operative in cui l'esercizio delle facoltà previste dal codice di procedura siano agevolmente azionabili e non vengano compresse dall'apparente evasione dell'onere motivazionale richiesto per l'adozione di misure cautelari reali.

In tale contesto, occorre riconoscere un'autonoma dignità processuale alla fase di selezione del materiale pertinente con le finalità investigative, costruendo una procedura operativa di applicazione generale e prevedendo modalità operative flessibili e adattabili alle esigenze probatorie di ciascun accertamento.

Una delle possibili soluzioni alla fumosità delle modalità operative adottate nella selezione di dati informatici in ambito giudiziario potrebbe essere individuata nell'inserimento di una procedura speciale che, combinando i principi e le linee guida dello standard ISO/IEC 27037 e 27050, consenta di acquisire le fonti di prova informatica secondo i principi dell'informatica forense e di esaminarli mediante le tecniche fornite dall'e-*discovery*, in un processo di elaborazione della fonte di prova informatica trasparente e verificabile.

Simile obiettivo potrebbe essere realizzato dall'adozione di un algoritmo operativo articolato nelle seguenti operazioni, eseguite garantendo la piena partecipazione delle parti processuali:

- acquisizione integrale dei supporti potenzialmente rilevanti secondo i principi dell'informatica forense, a garanzia della genuinità, integrità ed immodificabilità del contenuto acquisito;
- definizione in contraddittorio dei parametri di indicizzazione e dei criteri di ricerca da adottare per la selezione del materiale per-

[32] Di recente divulgazione la nota d'indirizzo organizzativo diramata dalla Procura Generale della Repubblica di Trento che recepisce il protocollo operativo proposto, uniformando le prassi in uso negli accertamenti tecnici di informatica forense ed adeguandole alle diverse esigenze processuali.

tinente e rilevante; l'esigenza del contraddittorio deriva dalla necessità di consentire non tanto il controllo quanto di favorire anche la permanenza di dati utili per le difese;
- formazione di una copia forense dei dati selezionati in quanto pertinenti e rilevanti per l'oggetto dell'accertamento;
- restituzione della copia forense integrale del supporto acquisito al legittimo utilizzatore.

Nell'esecuzione delle attività previste per ciascuna delle operazioni individuate nella procedura descritta, occorre considerare con particolare attenzione la cornice temporale entro la quale completare tutte le operazioni richieste, che non potranno protrarsi *sine die*, e le modalità di conservazione e gestione degli accessi al contenuto integrale dei supporti acquisiti.

In quest'ottica, la partecipazione alle attività tecniche dei soggetti coinvolti nelle forme più ampie riconosciute dall'ordinamento (accertamento tecnico non ripetibile o, meglio, incidente probatorio) appare elemento indefettibile della procedura proposta, consentendo di bilanciare adeguatamente le esigenze difensive tutelate in ambito penale e permettendo di verificare la legittimità delle operazioni eseguite e la proporzionalità delle misure, dei criteri e del materiale estratto dalla procedura adottata.