Capitolo II

Sequestro probatorio (art. 253 c.p.p.)

Focus sulla riforma: *la Legge 27 settembre 2021, n. 134 non ha dettato criteri direttivi in tema di sequestro probatorio.*

Giurisprudenza

«*In tema di sequestro probatorio di dispositivi informatici o telematici, l'estrazione di copia integrale dei dati in essi contenuti realizza solo una copia-mezzo, che consente la restituzione del dispositivo, ma non legittima il trattenimento della totalità delle informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede. (In motivazione, la Corte ha precisato che il pubblico ministero è tenuto a predisporre un'adeguata organizzazione per compiere tale selezione nel tempo più breve possibile, soprattutto nel caso in cui i dati siano sequestrati a persone estranee al reato, e provvedere, all'esito, alla restituzione della copia-integrale agli aventi diritto*», **Cass. pen., Sez. VI, 22 settembre 2020, n. 34265**.

Principio di proporzionalità e onere di motivazione del sequestro probatorio

Marco Pittiruti

SOMMARIO: 1. Nuovi itinerari giurisprudenziali in tema di sequestro probatorio. – 2. Le modalità acquisitive dei dati informatici o telematici. – 3. Un *vademecum* per il pubblico ministero nelle indagini in ambiente digitale. – 4. Garanzie partecipative e acquisizioni probatorie digitali.

1. *Nuovi itinerari giurisprudenziali in tema di sequestro probatorio*

Il tema delle acquisizioni probatorie di dati digitali ha conosciuto, negli ultimi anni, profonde innovazioni a livello giurisprudenziale. In particolare, mentre le prime esegesi relative al sequestro probatorio di materiale informatico offerte dalla Corte di Cassazione avallavano esplicitamente forme di *inquisitio generalis,* giacché si professava la legittimità di un'ablazione *sine die* dell'intero contenuto di sistemi informatici e telematici a fini investigativi [1], di recente, si sono progressivamente registrati orientamenti diversi, volti a introdurre precisi limiti alle attività di ricerca della prova del pubblico ministero a precipua tutela del soggetto *target* dell'attività investigativa [2]. Segno, dunque, di una rinnovata sensibilità per il valore della tutela della riservatezza nell'ambito delle indagini informatiche.

Ne rappresenta un'incontestabile riprova, da ultimo, la sentenza del 22 settembre 2020, n. 34625 [3], con la quale la Corte di Cassazione è stata chiamata a

---

[1] V., *ex multis*, Cass., Sez. VI, 29 gennaio 1998, Sarnataro, in *CED Cass.*, rv. 210820; Id., Sez. III, 18 marzo 2009, Apicella, *ivi*, rv. 243758; più di recente, cfr. anche Id., Sez. V, 14 marzo 2017, Storari, *ivi*, rv. 270018.

[2] Tali diverse esegesi si sono riscontrate, inizialmente, nell'ambito di procedimenti nei quali il sequestro probatorio aveva interessato strumentazione informatica in uso a giornalisti. Cfr. Cass., Sez. I, 16 febbraio 2007, Pomarici, in *Guida dir.*, 2007, n. 31, p. 57 ss., con nota di A. CISTERNA, *Ricerca da circoscrivere a singoli oggetti per evitare "irragionevoli intrusioni"*; in *Dir. inf.*, 2008, p. 731 ss., con nota di L. BACCHINI, *Il sequestro probatorio nei confronti del giornalista non indagato: il problema del bilanciamento di interessi costituzionalmente garantiti ed il rischio di elusione delle tutele*; in *Cass. pen.*, 2008, p. 2946 ss., con nota di A. LOGLI, *Sequestro probatorio di un personal computer. Misure* ad explorandum *e tutela della corrispondenza elettronica*; in *Dir. pen. proc.*, 2008, p. 765 ss., con nota di P. TROISI, *Sequestro probatorio del* computer *e segreto giornalistico*; Cass., Sez. VI, 31 maggio 2007, Sarzanini, in *Giur. it.*, 2008, c. 731 ss., con nota di C. GABRIELLI, *Quando il sequestro probatorio ha per oggetto l'*hard-disk *del computer di un giornalista*; in *Dir. pen. proc.*, 2008, p. 1416 ss., con nota di A. MACRILLÒ, *Segreto* ex *art. 200 c.p.p. e sequestro del* computer *in uso al giornalista*; Cass., Sez. VI, 15 aprile 2014, Minniti, in *Dir. pen. proc.*, 2015, p. 555 ss., con nota di F. PORCU, *Sequestro probatorio e segreto giornalistico: crocevia fra processo penale e informazione*; in *Cass. pen.*, 2015, p. 226 ss., con nota di G. BARBARA, *La motivazione dell'ordine di esibizione rivolto al giornalista* ex *art. 256 c.p.p. e del successivo provvedimento di sequestro*; Cass., Sez. VI, 24 febbraio 2015, Rizzo, in *Giur. it*., 2015, p. 1504 ss., con nota di S. LORUSSO, *Sequestro probatorio e tutela del segreto giornalistico*; in *Arch. n. proc. pen*., 2016, p. 269 ss., con nota di C. COSTANZI, *Perquisizione e sequestro informatico. L'interesse al riesame nel caso di estrazione di copie digitali e restituzione dell'originale*; in *Cass. pen*., 2016, p. 286 ss., con nota di G. SCHENA, *Ancora sul sequestro di materiale informatico nei confronti di un giornalista*.

[3] Per alcuni commenti alla pronuncia, v. A. DEL GIUDICE, *La Cassazione sul sequestro probatorio informatico: non si guardi al contenitore, ma al contenuto!*, in *Foro it.*, 2021, n. 6, II, p. 416; B.M. LEUZZI, *L'estrazione della copia integrale dei dati contenuti in dispositivi informatici realizza solo una copia-mezzo*, in *Cass. pen.*, 2021, p. 1001 ss.; M.R. MAGLIULO, *Illegittimo il trattenimento prolungato della copia integrale dei dati informatici in caso di sequestro probatorio*, in *Proc.*

pronunciarsi sul tema – di grande attualità, oltre che carico di importanti risvolti pratici per le indagini in ambiente digitale – delle modalità operative e dei limiti del sequestro probatorio di materiale digitale.

La vicenda in esame prendeva le mosse da un'attività investigativa volta ad accertare i reati di finanziamento illecito ai partiti e di traffico di influenze illecite di cui si sarebbe reso responsabile il presidente di una fondazione. Al fine di – così motivava il decreto – approfondire i rapporti intercorrenti tra quest'ultimo e i finanziatori della fondazione medesima, il pubblico ministero disponeva la perquisizione e il successivo sequestro probatorio di telefoni cellulari, *personal computer* portatili, dispositivi informatici e chiavette *USB* in uso a terzi estranei alle indagini.

Una volta sequestrate "fisicamente" le attrezzature informatiche, la pubblica accusa incaricava un consulente tecnico affinché procedesse alla duplicazione dei supporti informatici, «selezionando il materiale ritenuto probatoriamente rilevante rispetto ai reati contestati […] attraverso una ricerca eseguita mediante parole chiave, che si riservava di indicare al consulente», disponendo, altresì, la restituzione dei reperti informatici all'esito della duplicazione. In seguito, con provvedimento integrativo, il pubblico ministero precisava l'incarico del consulente, sollecitandolo, «ferma restando la selezione e l'estrazione di copia di *mail* e di messaggi (sotto qualsiasi forma ricevuti o trasmessi) e l'esame preliminare del reperto della polizia giudiziaria delegata», a selezionare ed estrarre dai reperti informatici in sequestro «copia dei documenti […] individuati tramite chiavi di ricerca specificatamente individuate».

Tempestivamente impugnato dalle persone a cui le *res* informatiche erano state sequestrate, il provvedimento ablativo veniva confermato dai giudici del riesame. Pertanto, gli interessati adivano la Corte di Cassazione, lamentando, in estrema sintesi, l'illegittimità del decreto sotto il profilo, per un verso, della mancanza del nesso di pertinenzialità tra la strumentazione informatica appresa e i reati ipotizzati dalla pubblica accusa, nonché, per altro verso, della violazione dei principi di adeguatezza e proporzionalità che necessariamente devono improntare ogni misura ablativa reale. Infine, si eccepiva l'assoluta genericità delle chiavi di ricerca individuate dal pubblico ministero al fine di delimitare il provvedimento di sequestro; quest'ultimo sarebbe stato, al contrario, impiegato quale indebito mezzo di reperimento di nuove *notitiae criminis*, come dimostrato dalla mancata restituzione del duplicato informatico contenente la totalità dei *file* appresi.

Nell'accogliere le doglianze difensive, i giudici di legittimità hanno affer-

pen. giust., 3/2021, p. 640 ss. Cfr., inoltre, volendo, M. PITTIRUTI, *Dalla Corte di cassazione un* vademecum *sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali* omnibus, in *www.sistemapenale.it*, 14 gennaio 2021.

mato che, qualora il vincolo probatorio su materiale digitale sia realizzato attraverso l'ablazione "fisica" delle memorie informatiche, dapprima occorre creare una copia integrale del contenuto della strumentazione appresa, funzionale alla restituzione di quest'ultima al legittimo titolare. Successivamente, la copia integrale così ottenuta va sottoposta ad analisi per selezionare i contenuti informativi pertinenti al reato per cui si procede. All'esito di tale selezione, la copia integrale – significativamente denominata dalla Suprema Corte «copia mezzo» – dev'essere restituita agli aventi diritto, poiché essa non rileva, di per sé, quale cosa pertinente al reato, trattandosi di «un insieme di dati indistinti e magmatici». Dal canto suo, il pubblico ministero può trattenere la copia integrale soltanto per il tempo strettamente necessario all'operazione di selezione, dovendo, di conseguenza, predisporre un'adeguata organizzazione per compiere tale attività nel più breve tempo possibile.

2. *Le modalità acquisitive dei dati informatici o telematici*

Al fine di comprendere i termini della questione e la linea ermeneutica seguita dalla Corte di Cassazione, pare opportuno soffermarsi sulle modalità di apprensione dei dati informatici contemplate, a seguito delle interpolazioni della Legge n. 48/2008[4], dal codice di rito[5]. Come noto, la riforma in parola non ha stabilito specifiche regole operative per l'acquisizione della *digital evidence*[6], dettando, al contrario, unicamente i canoni – variamente enunciati in diverse disposizioni del codice ma in ultimo riassumibili nell'endiadi genuinità e immodificabilità – ritenuti fondamentali per l'attività di ricerca della prova digitale[7].

---

[4] Legge 18 marzo 2008, n. 48, *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*, in *Gazz. Uff.*, 4 aprile 2008, n. 80 – Suppl. ord. n. 79.

[5] In tema, a livello monografico, v. A. TESTAGUZZA, Digital forensics. *Informatica giuridica e processo penale*, Wolters Kluwer-Cedam, Milano, 2015; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018; nonché, volendo, v. M. PITTIRUTI, Digital Evidence *e procedimento penale*, Giappichelli, Torino, 2017.

[6] Secondo Cass., Sez. III, 17 settembre 2015, R.G., in *CED Cass.*, rv. 265180, non avendo il legislatore tipizzato le misure tecniche e le procedure da impiegare per assicurare la genuinità del dato digitale, non è necessario da parte di colui che compie le analisi di *digital forensics* indicare il valore *hash* dei dati digitali acquisiti al fine di validarne l'autenticità.

[7] Cfr. L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4517 ss. La portata innovativa della riforma operata con la Legge n. 48/2008 è stata, tuttavia, depotenziata da un granitico orientamento giurisprudenziale, a parere del quale le *regulae iuris* introdotte dalla novella in discorso avrebbero valore solo "programmatico", rappresentando esclusivamente uno «stimolo alla professionalità della polizia giudiziaria operante» (così, *ex multis*, Cass.,

Era destinata, così, a restare irrisolta la questione, emersa fin dalle prime pioneristiche indagini informatiche[8], relativa alle modalità esecutive del sequestro di materiale informatico, con particolare riferimento al duplice interrogativo circa l'oggetto dell'acquisizione e le attività tecniche da compiersi. Eppure, già anteriormente alla novella, la dottrina aveva fermamente censurato la diffusa prassi, avallata dalla giurisprudenza di legittimità, di indiscriminata apprensione del materiale informatico a prescindere dall'effettivo nesso pertinenziale tra *res* e ipotesi di reato[9]. Segnatamente, quanto al *personal computer,* l'ablazione dell'intero sistema veniva giustificata valorizzando alternativamente la natura di corpo del reato o cosa pertinente al reato di quest'ultimo[10],

---

Sez. II, 21 ottobre 2020, n. 35447, *inedita*; in tale direzione v. anche Cass., Sez. V, 3 marzo 2017, La Rosa, in *CED Cass.*, rv. 270139). Pertanto, secondo questa esegesi, eventuali condotte scorrette nel reperimento e nell'acquisizione della prova digitale non riverberano sull'utilizzabilità della prova; all'opposto, è sufficiente che il giudice valuti in concreto la sussistenza di eventuali alterazioni dei dati originali e la conformità a questi ultimi delle informazioni estratte. In altre parole, eventuali condotte scorrette di acquisizione del dato digitale non comporterebbero l'inutilizzabilità della prova, ma rileverebbero solo sullo scivoloso versante del libero convincimento del giudice. Tale conclusione suscita, però, qualche perplessità. Difatti, a confutazione della tesi giurisprudenziale secondo cui i canoni di genuinità e non alterazione del dato informatico rappresenterebbero «prescrizioni meramente indicative, la cui inosservanza non è prevista a pena di nullità» (Cass., Sez. III, 19 aprile 2012, Zanetti, inedita), può rimarcarsi che lo svilimento della Legge n. 48/2008 al rango di *lex imperfecta* appare dimenticare che l'impiego di metodi di acquisizione scorretti muta la natura stessa della prova (digitale), la quale perde, una volta per tutte, l'idoneità a provare alcunché, in quanto irrimediabilmente contaminata. Alla luce di tali precisazioni, pertanto, sembra più opportuno configurare i canoni di genuinità e non alterazione della prova legislativamente imposti dalla Legge n. 48/2008 non già quali mere indicazioni operative prive di alcuna sanzione, ma veri e propri divieti impliciti presidiati dalla sanzione dell'inutilizzabilità. Ciò, anche in ossequio alla *ratio* delle interpolazioni operate dalla Legge n. 48/2008, vale a dire offrire una tutela più avanzata per la genuinità dell'informazione probatoria, a salvaguardia della attendibilità dell'accertamento. In tema, sia consentito rinviare, anche per le opportune annotazioni bibliografiche, a M. PITTIRUTI, Digital Evidence *e procedimento penale*, cit., p. 155 ss.

[8] Come, ad esempio, il sequestro di numerose *Bulletin Board System* avvenuto nel maggio 1994, nell'ambito dell'operazione investigativa denominata "*Hardware 1*". Cfr. G. ZICCARDI, *Informatica giuridica*, Giuffrè, Milano, 2011, vol. 1, p. 95 ss.

[9] Ne riferisce A. MONTI, *No ai sequestri indiscriminati di* computer, in *Dir. internet*, 2007, p. 268 ss., il quale configura, ironicamente, un «"principio di precauzione": non sapendo bene con cosa si ha a che fare, meglio eccedere e prendere tutto ciò che – genericamente – ricade nella nozione di *hardware*». V. anche ID., *Casi e problemi del sequestro informatico anche a distanza*, in G. CASSANO-S. PREVITI (a cura di), *Il diritto di Internet nell'era digitale*, Giuffrè, Milano, 2020, p. 955 ss., nonché G. DA VALLE, *L. 18.3.2008, n. 48 (Criminalità informatica) – Art. 9*, in *Legisl. pen.*, 2008, p. 297 ss.

[10] Cfr. Cass., Sez. III, 6 novembre 2002, Maggiore, in *Guida dir.*, n. 3, 2003, p. 79, ove si afferma laconicamente, nell'ambito di un'indagine in tema di pedopornografia *online*, che il *computer* dell'indagato, essendo stato usato per la consumazione del reato, costituisce corpo del reato «in quanto contenent[e] le immagini oscene oggetto dell'illecito acquisto o, comunque, ponendosi in plausibile rapporto di pertinenzialità con lo stesso».

ovvero l'esigenza di tutelare eventuali necessità probatorie legate all'opportunità di ricerche più approfondite sull'attrezzatura [11].

Simili conclusioni, frutto dell'elaborazione giurisprudenziale relativa al sequestro probatorio di grandezze "fisiche", scontano premesse di non adeguata solidità una volta mutuate sul terreno della prova digitale [12]. La necessità di approntare tutele ulteriori, rispetto alla apprensione di corpi fisici, per garantire l'integrità probatoria rappresenta un *leit motiv* delle indagini informatiche, giustificato dai caratteri peculiari del dato da apprendere: difatti, quest'ultimo consta di «impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intellegibili» [13]. L'impalpabilità del dato, allora, conferisce a quest'ultimo i connotati della volatilità e fragilità, con correlativo aumento del rischio di dispersione dell'informazione [14].

Non solo. Poiché ogni strumentazione informatica può contenere un'elevata quantità di informazioni [15], ne discende il pericolo di attività investigative "esplorative" [16]. A ciò consegue, quale corollario, l'ineludibile necessità di una tutela rafforzata per la sfera dei diritti dell'individuo coinvolto nell'attività d'indagine [17].

Da quest'ultimo angolo visuale, può scorgersi un ulteriore aspetto critico della normativa dettata dalla Legge n. 48/2008. Nell'ambito delle norme che disciplinano le attività a iniziativa della polizia giudiziaria, il legislatore ha espresso un chiaro *favor* per una preliminare selezione dei dati rilevanti custo-

---

[11] V. Cass., Sez. V, 3 aprile 2006, Ferro, *inedita*.

[12] Per una panoramica sui caratteri del dato digitale, v. G. PAOLOZZI, *Relazione introduttiva*, in L. LUPÁRIA-L. MARAFIOTI-G. PAOLOZZI (a cura di), *Dimensione tecnologica e prova penale*, Giappichelli, Torino, 2019, p. 1 ss.

[13] Così M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 284.

[14] Per il rilievo secondo cui «immaterialità ed alterabilità sono connotati intrinseci dei dati trasmessi in un linguaggio digitale», v. R. DEL COCO, *L'utilizzo probatorio dei dati* whatsapp *tra lacune normative e avanguardie giurisprudenziali*, in *Proc. pen. giust*, 3/2018, p. 533. Sul legame tra immaterialità e fragilità del dato informatico, v. P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 401 ss., nonché, da ultimo, G. FIORELLI, *Lo* screenshot *quale prova documentale: regole acquisitive e garanzie di affidabilità*, in *Dir. internet*, 2020, p. 507.

[15] F. SIRACUSANO, *La prova digitale transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Proc. pen. giust.*, 1/2017, p. 179, nt. 4, evidenzia la «profonda sproporzione fra le prove digitali e i loro recipienti: piccolissimi supporti informatici (si pensi alle chiavette *Usb*) sono in grado di accogliere al loro interno una grandissima quantità di informazioni».

[16] Cfr. Cass., Sez. IV, 17 aprile 2012, soc. Ryanair, in *Cass. pen.*, 2013, p. 1523 ss., con nota di G. BONO, *Illegittimità dei provvedimenti di perquisizione e sequestro delle credenziali di accesso al sistema di prenotazione di voli aerei* on line, nonché in *Dir. inf.*, 2012, p. 1148 ss., con nota di G. CORRIAS LUCENTE, *Perquisizione e sequestro informatici: divieto di* inquisitio generalis.

[17] V., in tema, V. GRAMUGLIA, *Sequestro probatorio del reperto digitale e manifestazioni distorsive dell'attività di indagine*, in *Dir. internet*, 2021, p. 745 ss.

diti nel sistema informatico-obiettivo dell'attività d'indagine, dal momento che si prevede una perquisizione del dispositivo da parte degli ufficiali di polizia giudiziaria (art. 352, comma 1-*bis,* c.p.p.), eventualmente assistiti da esperti di *digital forensics* (art. 348, comma 4, c.p.p.), cui deve far seguito il sequestro "selettivo" dei dati digitali contenenti informazioni pertinenti al reato (art. 354, comma 2, c.p.p.).

Le cose stanno diversamente, invece, nel caso di sequestro disposto ai sensi dell'art. 253 c.p.p. dal pubblico ministero. Invero, i riferimenti alla duplicazione mediante copia forense (o *bit-stream image*)[18] contenuti negli artt. 254-*bis* e 260 c.p.p. sembrerebbero imporre agli operanti la previa apprensione dell'intero contenuto del sistema informatico d'interesse[19], declinabile secondo due diverse modalità tra loro alternative: la duplicazione del sistema realizzata direttamente in sede d'esecuzione del provvedimento ablativo, oppure, come verificatosi nel caso di specie, l'apprensione "fisica" delle memorie, cui segue la loro duplicazione in laboratorio finalizzata all'analisi e alla selezione dei contenuti informativi rilevanti per l'indagine.

Tuttavia, non ci vuole troppo senso pratico per rendersi conto che, in entrambe le ipotesi ora menzionate, mediante l'acquisizione del duplicato informatico della strumentazione sequestrata nella sua interezza, gli investigatori vengono a contatto con una notevole mole di dati non pertinenti al reato per cui si procede. Il che implica un'ingiustificata compressione del diritto alla riservatezza del soggetto che subisce l'"intrusione" informatica[20].

Inoltre, onde poter "estrarre" le informazioni rilevanti ai fini dell'accertamento, la pubblica accusa deve compiere attività tecniche non espressamente disciplinate dal codice di rito, con particolare riguardo alla durata delle operazioni[21]. Ogni tutela per il legittimo titolare del bene informatico sequestrato

---

[18] La *bit stream image*, o copia forense, consiste in una perfetta riproduzione, *bit* per *bit*, di un qualsiasi dispositivo di riproduzione. Tale opera di clonazione riguarda tutte le aree del disco, comprese quelle che non contengono alcun *file* visibile all'utente (aree non allocate), il che permette il recupero di *file* (o porzioni di esso) cancellati. Cfr. M. FERRAZZANO-L. SUMMA, *La selezione dei dati informatici in ambito giudiziario: prassi e modalità operative*, in R. BRIGHI (a cura di), *Nuove questioni di informatica forense*, Aracne, Roma, 2022, p. 61 ss.

[19] Nel senso del testo, Cass., Sez. VI, 12 febbraio 2014, Genchi, in *CED Cass.*, rv. 259782.

[20] Sulla tutela della riservatezza informatica nel corso delle indagini in ambiente digitale cfr. F. PALMIOTTO, *Le indagini informatiche e la tutela della riservatezza informatica*, in *www.la legislazionepenale.eu*, 1° luglio 2019.

[21] Secondo la giurisprudenza, l'espletamento dell'attività di analisi da parte dell'ausiliario oltre il termine di durata delle indagini preliminari sul materiale informatico tempestivamente posto in sequestro ed acquisito impedisce l'acquisizione in via diretta al fascicolo del dibattimento dei risultati, ma non osta alla loro utilizzazione a seguito dell'esame dello stesso ausiliario effettuato nel contraddittorio delle parti. Cfr. Cass., Sez. III, 6 giugno 2019, Rigano, in *CED Cass.*, rv. 277164.

resta, così, affidata all'art. 262 c.p.p., il quale si limita laconicamente a subordinare il diritto alla restituzione del bene alla circostanza che «non è necessario mantenere il sequestro a fini di prova», senza vieppiù chiarire se il diritto alla restituzione in capo al legittimo titolare si limiti al bene "fisico" che contiene il dato informatico (quale il *personal computer* o la chiavetta *usb* sottoposta a sequestro) o, viceversa, si estenda alla copia-clone del sistema.

3. *Un* vademecum *per il pubblico ministero nelle indagini in ambiente digitale*

La sentenza in commento si fa carico di porre rimedio al rilevato *deficit* di genericità del testo normativo, dettando una sorta di *vademecum* per il pubblico ministero in tema di acquisizioni probatorie informatiche, con precipuo riguardo, da un lato, all'onere motivazionale che deve sorreggere il decreto di sequestro e, dall'altro lato, alle operazioni tecniche da compiere sul dato digitale sequestrato.

Punto di partenza dello sforzo argomentativo della Corte di Cassazione sono i recenti approdi della giurisprudenza di legittimità in tema di motivazione del decreto di sequestro probatorio. Invero, i giudici di legittimità rimarcano che «la portata precettiva degli artt. 42 Cost. e 1 del primo Protocollo addizionale della Convenzione Edu richiede che le ragioni probatorie del vincolo di temporanea indisponibilità della cosa […] siano esplicitate nel provvedimento giudiziario con adeguata motivazione, allo scopo di garantire che la misura, a fronte delle contestazioni difensive, sia soggetta al permanente controllo di legalità – anche sotto il profilo procedimentale – e di concreta idoneità in ordine all'*an* e alla sua durata, in particolare per l'aspetto del giusto equilibrio o del ragionevole rapporto di proporzionalità tra il mezzo impiegato, ovvero lo spossessamento del bene, e il fine endoprocessuale perseguito, ovvero l'accertamento del fatto di reato»[22].

[22] Sull'onere di motivazione del decreto di sequestro probatorio, da ultimo, nel senso che esso «deve contenere una motivazione che, per quanto concisa, dia conto specificatamente della finalità perseguita per l'accertamento dei fatti», v. Cass., Sez. Un., 19 aprile 2018, Botticelli, in *Cass. pen*., 2018, p. 4088 ss., con nota di G. SCHENA, *Quello che le Sezioni unite non dicono a proposito di "idoneità della motivazione" nel caso di sequestro probatorio del* corpus delicti; in *Dir. pen. cont. – Riv. trim.*, 2018, n. 9, p. 69 ss., con nota di V. GRAMUGLIA, *Le Sezioni Unite tornano sui confini dell'onere di motivazione del decreto di sequestro probatorio del* corpus delicti; in *Dir. pen. proc.*, 2019, p. 228 ss., con nota di M.F. CORTESI, *Sequestro del corpo del reato e onere motivazionale: dopo un tormentato dibattito interpretativo raggiunto "forse" un punto fermo*. V. anche Cass., Sez. II, 17 settembre 2021, Cristofori, in *CED Cass.*, rv. 282200, secondo cui il decreto di sequestro probatorio di cosa pertinente al reato deve indicare, oltre che la rile-

Proprio sul necessario rapporto di proporzionalità tra *res* appresa e finalità investigative si incentra il ragionamento della Suprema Corte. Sulla scia delle numerose sentenze che, in tempi recenti, hanno impiegato i canoni di adeguatezza e proporzionalità quali parametri di legittimità del sequestro probatorio informatico [23], la pronuncia in commento si spinge sino a elevare il principio di proporzione ad architrave fondante del sistema processuale, di importanza tale da travalicare «il perimetro della libertà individuale per divenire termine necessario di raffronto tra la compressione dei diritti quesiti e la giustificazione della loro limitazione».

Ciò si desume, a parere della Corte, dalle fonti dell'Unione Europea, tra cui l'art. 5, par. 3 e 4 del T.U.E., nonché gli artt. 49, par. 3, e 52, par. 1, della Carta dei diritti fondamentali, e trova significativa conferma nella giurisprudenza della Corte costituzionale [24], da cui può ricavarsi l'insegnamento che «il generale controllo di ragionevolezza, a sua volta effettuato attraverso il bilanciamento tra gli interessi in conflitto, comprend[e] il canone modale della proporzionalità». In altre parole, il principio di proporzionalità assume il ruolo di limite funzionale dell'attività della pubblica accusa, a tutela dell'indagato e dei terzi interessati dall'indagine [25]. Tanto da far preconizzare ai giudici di legittimità che il medesimo principio assumerà il ruolo di «guida per lo sviluppo futuro della materia dei diritti fondamentali» [26].

A ben vedere, l'opzione esegetica privilegiata dalla Suprema Corte trova significative conferme anche nel codice di rito. Si allude, in particolare, all'art. 224-*bis*, comma 5, c.p.p., il quale disciplina le operazioni peritali che richiedano il compimento di atti idonei a incidere sulla libertà personale, quali il pre-

---

vanza della *res* ai fini dell'accertamento dei fatti, anche il nesso di derivazione e di pertinenza della cosa con il reato; in mancanza, il provvedimento di sequestro è affetto da nullità genetica non sanabile in sede di riesame.

[23] *Ex multis*, possono richiamarsi Cass., Sez. VI, 2 luglio 2019, soc. Magiste s.r.l., in *Dir. internet*, 2019, p. 775 ss.; Cass., Sez. VI, 24 ottobre 2019, Scarsini, in *Proc. pen. giust.*, 3/2020, p. 660 ss., con nota di L. NULLO, *Sequestro probatorio di materiale documentativo e principi di adeguatezza e proporzionalità*.

[24] La sentenza in commento richiama, in particolare, Corte cost., sentenza 9 maggio 2013, n. 85, in *Gazz. Uff.*, 15 maggio 2013, n. 20, nonché Corte cost., sentenza 24 gennaio 2017, n. 20, in *Gazz. Uff.*, 1° febbraio 2017, n. 5.

[25] In dottrina, sul principio in discorso, in una prospettiva più generale, v. M. CAIANIELLO, *Il principio di proporzionalità nel processo penale*, in *Dir. pen. cont. – Riv. trim.*, 2014, nn. 3-4, p. 143 ss. Con specifico riguardo alla prova tecnologica, v. F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Dir. pen. cont. – Riv. trim*, 2018, n. 2, p. 176 ss., nonché L. TAVASSI, *Acquisizione di tabulati, tutela della* privacy *e rispetto del principio di proporzionalità*, in *Arch. pen.* web, 2022, n. 2.

[26] In dottrina, v. P. FELICIONI, *L'acquisizione di contenuti* e-mail *e delle* chat whatsapp *tra intercettazioni e sequestro*, in *Riv. G.d.F.*, 2019, p. 1578.

lievo di capelli, di peli o di mucosa del cavo orale su persone viventi ai fini della determinazione del profilo del DNA o di accertamenti medici[27]. Ai sensi della disposizione in parola, infatti, a parità di risultato, la scelta tra le diverse tecniche da impiegare per compiere l'accertamento deve orientarsi a favore di quelle meno invasive per il *target* delle operazioni.

Applicando tali coordinate al tema oggetto di scrutinio, il principio di proporzionalità dell'azione consente di comporre armonicamente la doverosa tutela per i diritti individuali con le esigenze legate all'efficacia dell'accertamento[28]. Se è vero che è certamente possibile, in astratto, un sequestro *omnibus* disposto dal pubblico ministero, ovverosia afferente all'intera strumentazione informatica in uso a un determinato soggetto, è altrettanto vero che simile approccio è legittimo soltanto in casi peculiari: segnatamente, qualora ragioni di salvaguardia delle esigenze legate all'accertamento – si pensi alla natura del bene o alla difficoltà di individuazione della *res* – siano tali da imporre una rimodulazione del principio del minor sacrificio necessario[29].

---

[27] Sul tema, diffusamente, v. L. MARAFIOTI-L. LUPÁRIA (a cura di), *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del Trattato di Prüm, istitutiva del database genetico nazionale e recante modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85)*, Giuffrè, Milano, 2010. Con specifico riferimento al tema dei prelievi biologici, cfr. R. DEL COCO, *Il prelievo dei campioni biologici (art. 9)*, *ivi*, p. 61 ss.

[28] In dottrina, sul tema, v. M. TORRE, *Indagini informatiche e principio di proporzionalità*, in *Proc. pen. giust.*, 6/2019, p. 1433 ss.; L. ALGERI, *Principio di proporzionalità e sequestro probatorio di sistemi informatici*, in *Dir. pen. proc.*, 2020, p. 849 ss.; C. PARODI, *Il sequestro probatorio dei dispositivi informatici: necessario contemperare esigenze investigative e principio di proporzionalità*, in *www.ilpenalista.it*, 10 dicembre 2020; V. SISTO, *La tutela del segreto del giornalista in caso di perquisizione e sequestro di materiale informatico*, in *Proc. pen. giust.*, 5/2021, p. 1221 ss.; G. CASCONE, *Il sequestro informatico nel prisma del principio di proporzione*, in *Dir. pen. proc.*, 2022, p. 123 ss.; C. FONTANI, *Il sequestro probatorio di un documento informatico: bilanciamento tra esigenze investigative e baluardi difensivi*, in *Dir. pen. proc.*, 2022, p. 237 ss. Sia consentito, inoltre, rimandare a M. PITTIRUTI, *Adeguatezza e proporzionalità nel sequestro di un sistema informatico*, in *Dir. internet*, 2019, p. 777 ss.

[29] L'ablazione dell'intero contenuto del sistema informatico o telematico obiettivo dell'attività investigativa potrebbe, altresì, trovare giustificazione nella mera presenza di ostacoli all'accesso al dato, quale l'impiego di *password* o di tecniche crittografiche impiegate dall'utente, essendo impossibile selezionare il dato d'interesse al momento del primo contatto tra operanti e dato digitale. Ciò non significa, tuttavia, che debba sempre procedersi all'asportazione dell'intera strumentazione "fisica". Piuttosto, in tal caso, gli operanti – qualora tecnicamente possibile – dovranno procedere alla duplicazione mediante copia forense dell'intero sistema, affinché esso sia in seguito sottoposto ai doverosi accertamenti per la selezione dei soli dati di interesse investigativo. In quest'ottica, va censurata l'affermazione, di matrice giurisprudenziale, secondo cui il sequestro *omnibus* di materiale informatico attraverso l'ablazione fisica delle memorie trova giustificazione nell'indisponibilità di personale tecnico in grado di superare le protezioni legittimamente inserite dal proprietario dell'attrezzatura (cfr. Cass., Sez. VI, 2 luglio 2019, soc. Magiste s.r.l., cit.). Simile assunto, invero, risulta assai pericoloso, in quanto tale condizione, spesso ricorrente nella prassi, viene a far dipendere l'afflittività in concreto del sequestro probatorio del materiale digitale da con-

Pertanto, nella prospettiva privilegiata dalla Corte, in ossequio al canone secondo cui l'apposizione del vincolo dev'essere tale da non arrecare un inutile aggravio per il soggetto passivo dell'attività investigativa, un ruolo fondamentale va assegnato alla motivazione del sequestro. Essa funge, infatti, da «strument[o] "compensativ[o]" di garanzia per il soggetto che subisce la limitazione dei propri diritti». In quest'ottica, riprendendo argomenti già compiutamente sviluppati in altra recente pronuncia della medesima Sezione della Corte di Cassazione [30], la sentenza in esame individua tre profili – «quantitativo, qualitativo e temporale» – che devono essere, pena l'illegittimità del decreto di sequestro, oggetto di specifica motivazione da parte del pubblico ministero. Dunque, affinché il sequestro sia legittimo, occorre che il provvedimento sia specificamente motivato *a)* in ordine al nesso di pertinenza tra il bene appreso e l'ipotesi investigativa, *b)* in relazione alla tipologia di operazioni tecniche da svolgere sul dato, *c)* con riguardo alla durata temporale del vincolo [31].

tingenze organizzative e, segnatamente, da possibili lacune nella disponibilità del personale da parte della polizia giudiziaria. Da ultimo, sui rapporti tra prova digitale e *nemo tenetur se detegere*, v. A. MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici … e non solo*, in *Proc. pen. giust.*, 4/2021, p. 729 ss., nonché F.N. RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'auto-incriminazione*, in *Cass. pen.*, 2022, p. 880 ss.

[30] Cfr. Cass., Sez. VI, 4 marzo 2020, Scagliarini, in *CED Cass.*, rv. 279143. Tale pronuncia si segnala, altresì, in quanto la Suprema Corte ha sostenuto che non rientra nei poteri del Tribunale del riesame ordinare la distruzione dei dati "clonati" mediante estrazione di duplicato forense, potendo il collegio solo definire i limiti del vincolo reale, disponendone la restituzione della copia-mezzo all'avente diritto, consentendo, per tale via, il reintegro nel possesso esclusivo dei dati. V. anche Cass., Sez. V, 9 settembre 2019, Re, in *CED Cass.*, rv. 276908, secondo cui il Tribunale del riesame può legittimamente disporre, anche in assenza di una richiesta della pubblica accusa sul punto, la restituzione della strumentazione informatica oggetto di sequestro previa estrazione di copia forense.

[31] In ottica parzialmente diversa, però, v. Cass., Sez. I, 11 gennaio 2022, Gervasoni, in *CED Cass.*, rv. 282725, secondo cui sarebbe legittima la motivazione di un decreto di perquisizione e sequestro informatico *omnibus* imperniata sulla necessità di acquisire l'intera strumentazione di natura informatica in uso all'indagato, al fine di procedere alla duplicazione mediante copia forense e per controllare gli accessi e gli *account*, anche in relazione ai profili gestiti sui *social network*. Nel caso di specie, il fondato motivo che legittimava l'impiego di mezzi di ricerca della prova digitale nei confronti del ricorrente afferiva alla pubblicazione, mediante il proprio profilo *Twitter*, di commenti dal contenuto ingiurioso relativi al Presidente della Repubblica e ad altre figure istituzionali.

4. *Garanzie partecipative e acquisizioni probatorie digitali*

Tale inedita apertura in favore di un onere di motivazione "rafforzato", allorché il sequestro probatorio informatico sia realizzato mediante l'ablazione "fisica" del dispositivo, trova fondamento – a parere della Suprema Corte – nella promiscuità del dato digitale. Segnatamente, la necessità di chiarire, in sede di apposizione del vincolo, la continenza dell'attività ablativa rispetto ai fini endoprocedimentali deriva dal rischio, immanente in ogni attività d'investigazione informatica, di acquisizione "casuale" di informazioni «supersensibili», vale a dire attinenti alla «sfera privata e intima» dell'utilizzatore della strumentazione [32].

In questo passaggio si annida il "cuore" della pronuncia, la quale coraggiosamente si addentra in considerazioni informatico-forensi circa le attività che devono essere predisposte dal pubblico ministero, a tutela della riservatezza dell'interessato, una volta eseguito il sequestro.

Dopo aver chiarito che la procedura più adeguata a garantire l'integrità dei dati, in ossequio allo statuto della *digital evidence* coniato dalla Legge n. 48/2008, consiste nella creazione di una copia-clone dell'*hard disk* identica all'originale, la Corte di Cassazione evidenzia che tale copia (*rectius* duplicato) è solo "servente" alla selezione dei contenuti d'interesse investigativo e alla restituzione del bene al legittimo titolare [33]. Pertanto, i giudici di legittimità onerano il pubblico ministero di un passaggio successivo all'analisi della strumentazione informatica, vale a dire la restituzione della copia-clone [34]. Qualora ciò

---

[32] Analogo rischio era già stato adombrato da Cass., Sez. VI, 14 febbraio 2019, Guastalla, in *CED Cass.*, rv. 277372. Cfr. anche Cass., Sez. VI, 9 dicembre 2020, Pessotto, in *CED Cass.*, rv. 280838.

[33] Cfr. Cass., Sez. VI, 16 dicembre 2021, Antonucci, in *www.italgiure.giustizia.it/sncass*. Secondo i giudici di legittimità, il pubblico ministero è tenuto a predisporre una adeguata organizzazione per compiere la selezione dei dati digitali nel tempo più breve possibile, soprattutto nel caso in cui i dati siano stati sequestrati a persone estranee al reato per cui si procede; a seguito di tali operazioni di selezione, la copia integrale deve essere restituita agli aventi diritto. Ciò, tuttavia, non vale a coniare un termine perentorio – coincidente con la celebrazione dell'udienza di riesame del sequestro – la cui inosservanza produrrebbe effetti demolitori sul vincolo probatorio in essere. All'opposto, tali principi rivestirebbero una funzione strumentale, nella misura in cui demandano al Tribunale del riesame un accertamento in concreto, inevitabilmente legato alle peculiarità del caso concreto, «finalizzato a verificare se le operazioni di selezione del materiale siano conformi alla esigenza di differimento temporaneo della valutazione de nesso di pertinenza tra *res* e reato che si intenda provare ovvero si traducano in una elusione delle garanzie […], con conseguente violazione del diritto di proporzione e limitazione illegittima di diritti delle persone».

[34] In ordine alla *vexata quaestio* circa la possibilità di coltivare l'impugnazione del provvedimento ablativo a fronte della restituzione dei dati informatici ma non della copia-mezzo, cfr. Cass., Sez. V, 15 febbraio 2019, Pannella, in *Giur. it.*, 2019, c. 2286 ss., con nota di T. LINARDI,

non accadesse, sarebbe inevitabile «una elusione ed uno svuotamento della portata dell'art. 253, comma 1, c.p.p. che legittima il sequestro probatorio solo delle cose "necessarie" per l'accertamento dei fatti»[35].

Sotto questo profilo, le conclusioni cui sono pervenuti i giudici di legittimità appaiono perfettamente sintoniche con la nuova disciplina delle intercettazioni, frutto delle interpolazioni operate dal D.L. n. 161/2019[36], convertito con modificazioni dalla Legge n. 7/2020[37]. Come noto, il novellato art. 268, comma 2-*bis*, c.p.p. prevede che il pubblico ministero debba dare indicazioni

Il sequestro probatorio e la "copia" dei dati informatici, secondo cui «è inammissibile il ricorso per cassazione avverso l'ordinanza del tribunale del riesame di conferma del sequestro probatorio di un *computer* o di un supporto informatico, nel caso in cui ne risulti la restituzione previa estrazione di copia dei dati immagazzinati, qualora non venga dedotta, sulla base di elementi univoci, la lesione di interessi primari connessi all'indisponibilità delle informazioni contenute negli oggetti sequestrati, non essendo a tal fine sufficiente il mero interesse del ricorrente ad una pronunzia sulla legittimità del provvedimento […]». In proposito, le Sezioni Unite avevano già precisato che l'ammissibilità del ricorso per cassazione avverso il provvedimento del riesame che conferma il decreto di sequestro probatorio di strumentazione informatica, qualora quest'ultima sia già stata restituita, è subordinata alla deduzione di un interesse, concreto e attuale, alla esclusiva disponibilità dei dati. Cfr. Cass., Sez. Un., 20 luglio 2017, Andreucci, in *Cass. pen.*, 2017, p. 4303 ss., con nota di A. MARI, *Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione di copia dei dati*; *ivi*, 2018, p. 131 ss., con nota di P. RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico*; in *Arch. pen.* web, 2018, n. 1, con nota di L. BARTOLI, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*. Per un commento alla pronuncia, v. anche G. TODARO, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare:* revirement *delle Sezioni Unite*, in *Dir. pen. cont. – Riv. trim.*, 2017, n. 11, p. 157 ss. Sul medesimo tema, le Sezioni Unite avevano affermato, in precedenza, che, «una volta restituita la cosa sequestrata, la richiesta di riesame del sequestro, o l'eventuale ricorso per cassazione contro la decisione del tribunale del riesame è inammissibile per sopravvenuta carenza di interesse […], dal momento che il relativo provvedimento è autonomo rispetto al decreto di sequestro, né è soggetto ad alcuna forma di gravame, stante il principio di tassatività delle impugnazioni». V. Cass., Sez. Un., 24 aprile 2008, Tchmil, in *Cass. pen.*, 2008, p. 4031 ss., con nota di E. APRILE, *Carenza di interesse al riesame del sequestro probatorio di bene già restituito previa estrazione di copia*; in *Dir. pen. proc.*, 2009, p. 469 ss., con nota di S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare.*

[35] Cfr., in tema, Cass., Sez. VI, 24 febbraio 2015, Rizzo, cit. In tale pronuncia, la Suprema Corte ha evidenziato che le disposizioni introdotte dalla Legge n. 48/2008 riconoscono al dato informatico, in quanto tale, la caratteristica di oggetto del sequestro, di modo che la restituzione, previo trattenimento di copia, del supporto fisico di memorizzazione, non comporta il venir meno del sequestro giacché permane una perdita autonomamente valutabile per il titolare del dato. In termini, v. Cass., Sez. III, 23 giugno 2015, Cellino, in *Dir. pen. proc.*, 2016, p. 508 ss., con nota di V. ZAMPERINI, *Impugnabilità del sequestro probatorio di dati informatici.*

[36] Decreto-Legge 30 dicembre 2019, n. 161, *Modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni*, in *Gazz. Uff.*, 31 dicembre 2019, n. 305.

[37] Legge 28 febbraio 2020, n. 7, *Conversione in legge, con modificazioni, del decreto-legge 30 dicembre 2019, n. 161, recante modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni*, in *Gazz. Uff.*, 28 febbraio 2020, n. 50.

e vigilare affinché nei verbali relativi alle conversazioni captate non siano riportate espressioni lesive della reputazione delle persone o che riguardino dati personali sensibili, salvo che risultino rilevanti ai fini delle indagini. Ciò conforta nel ritenere indefettibile, più in generale, in ambito di indagini digitali una rigorosa selezione del materiale appreso, al fine di evitare indebite intrusioni nella sfera personalissima del soggetto *target* dell'attività investigativa non giustificate dalle esigenze dell'accertamento. Invero, sarebbe del tutto irragionevole ritenere possibile, attraverso un sequestro di materiale informatico o telematico, inserire nel fascicolo investigativo quei medesimi dati che, per espressa previsione legislativa, devono essere espunti dal fascicolo del pubblico ministero se acquisiti attraverso il meccanismo delle captazioni occulte. Proprio l'attività di selezione del dato utile alle indagini, al contrario, rappresenta passaggio essenziale – sia pur non previsto a livello legislativo – delle attività demandate all'accusa a seguito di un sequestro informatico [38].

In quest'ottica, la pronuncia sembra apportare nuova linfa al dibattito circa le garanzie partecipative assegnate alla difesa nell'ambito delle acquisizioni probatorie digitali. Difatti, non può sfuggire come la scansione trifasica dell'attività di acquisizione della *digital evidence* delineata dalla sentenza in commento (apprensione del contenitore/creazione di una copia forense in laboratorio/successiva estrazione dei soli dati rilevanti) susciti nuovi e pressanti interrogativi con particolare riferimento alla doverosità circa l'attivazione del congegno delineato dall'art. 360 c.p.p.

Sul punto, l'elaborazione scientifica ha sollecitato l'attivazione delle garanzie partecipative sin dalla fase investigativa, giacché sussisterebbe un concreto rischio di modifica del dato sottoposto ad analisi [39], mentre la giurisprudenza

[38] Nel medesimo senso anche la *Nota d'indirizzo organizzativo* della Procura Generale della Repubblica di Trento del 21 ottobre 2021, in *www.giurisprudenzapenale.com*, secondo cui «un riversamento agli atti del procedimento della copia forense nella sua interezza, comprendente anche *chat* o messaggi con contenuto irrilevante per il processo, implica, invece, un'inammissibile ed illecita diffusione di dati che attengono alla sfera personale, intima ed inviolabile di ogni individuo e non è assolutamente consentito, perché comporta, inevitabilmente, fra l'altro, la possibilità di divulgazione di fatti lesivi dell'onorabilità e della reputazione della persona, di dati penalmente irrilevanti che possono, però, risultare devastanti per la vita dei soggetti coinvolti (anche se estranei al procedimento) e che quando riguardano l'attività di operatori economici, rendendo conoscibili *know how* o strategie riservate d'impresa possono anche alterare l'ordinario andamento del mercato con grave danno per l'economia nazionale o di un determinato territorio, nonché la conoscibilità e tracciabilità di orientamenti politici, tendenze sessuali, convincimenti religiosi, rapporti sentimentali, dati sanitari e altri dati sensibili non solo della persona sottoposta ad indagini, ma anche di soggetti del tutto estranei e persino di minorenni».

[39] Sul tema, da ultimo, F. CERQUA, *Tra comunicazioni telematiche e rito: il sequestro della corrispondenza elettronica*, in L. LUPÁRIA-L. MARAFIOTI-G. PAOLOZZI (a cura di), *Dimensione tecnologica e prova penale*, cit., p. 105 ss.; ID., *Il sequestro della corrispondenza elettronica nel processo penale*, in G. CASSANO-S. PREVITI (a cura di), *Il diritto di Internet nell'era digitale*, cit.,

si è attestata nel senso di una generale ripetibilità delle attività di analisi sul dato informatico, sul presupposto della loro possibile reiterazione in sede dibattimentale [40].

A tal riguardo, sia pure quale *obiter dictum*, la sentenza in commento censura – sotto il profilo del mancato adempimento dell'onere motivazionale – la scelta della pubblica accusa di assegnare alla polizia giudiziaria l'esame preliminare della strumentazione informatica, giacché ciò comporterebbe un'ingiustificata lesione dei principi di adeguatezza e proporzionalità. Il che avvalora la tesi secondo cui le attività di duplicazione del dato digitale devono essere compiute nel contraddittorio tra le parti, essendo insussistente il pericolo che l'indagato disperda o cancelli le informazioni contenute nel supporto informatico, in quanto quest'ultimo non si trova più nella sua disponibilità. Si recupera, per tale via, l'insegnamento di quell'attenta dottrina che da tempo sottolinea il rischio, assai concreto, che qualsiasi operazione compiuta sul dato informatico si traduca in un'irreparabile modifica dello stesso, anche qualora si utilizzino i più moderni strumenti di *digital forensics* [41].

---

p. 915 ss.; A. BUZZELLI, *Perquisizione di spazi informatici e* preview, L. LUPÁRIA-L. MARAFIOTI-G. PAOLOZZI (a cura di), *Dimensione tecnologica e prova penale*, cit., p. 117 ss.

[40] Nel senso che nessun preavviso è dovuto al difensore allorché gli ufficiali di polizia giudiziaria intendano procedere alla duplicazione di dati informatici, poiché si tratterebbe di una «operazione meramente meccanica, riproducibile per un numero indefinito di volte», Cass., Sez. I, 20 aprile 2009, Corvino, in *CED Cass.*, rv. 244454. In termini analoghi, Cass., Sez. II, 19 febbraio 2015, Apicella, *ivi,* rv. 263797; Cass., Sez. II, 4 giugno 2015, Scanu, *ivi,* rv. 264286; Cass., Sez. II, 1° luglio 2015, Posanzini, in *CED Cass.*, rv. 264572; Cass., Sez. V, 21 marzo 2016, Branchi, in *Cass. pen.*, 2016, p. 4486 ss., con nota di F. Salviani; Cass., Sez. V, 6 luglio 2020, Barhoumi, in *Dir. internet*, 2020, p. 691 ss., con nota di V. GRAMUGLIA, *La natura (ir)ripetibile dell'attività d'indagine sul reperto digitale*; Cass., Sez. II, 27 novembre 2020, Lombardo, in *CED Cass.*, rv. 280618; Cass., Sez. I, 10 giugno 2021, Marziano, in *CED Cass.*, rv. 282072. In tema, cfr. anche Cass., Sez. I, 5 marzo 2009, Aversano Stabile, in *Dir. pen. proc.*, 2010, p. 337 ss., con nota di A.E. RICCI, Digital evidence *e irripetibilità delle operazioni acquisitive*. In tale occasione, la Suprema Corte stabiliva che «non rientra nel novero degli atti irripetibili l'attività di estrazione di copia di "*file*" da un *computer* oggetto di sequestro, dal momento che essa 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 comunque assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale».

[41] V., *ex multis*, L. LUPÁRIA, *La disciplina processuale e le garanzie difensive*, in L. LUPÁRIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Giuffrè, 2007, p. 151 ss.