Il presente volume è stato oggetto di procedura di doppio referaggio cieco (double blind peer review) *da parte di due* referee. *L'Editore conserva la relativa documentazione*

SILVIA SIGNORATO

LE INDAGINI DIGITALI

PROFILI STRUTTURALI DI UNA METAMORFOSI INVESTIGATIVA

G. GIAPPICHELLI EDITORE – TORINO

CAPITOLO IV
LE INDAGINI DIGITALI REPRESSIVE

SEZIONE PRIMA
ATTI INVESTIGATIVI TIPICI

SOMMARIO: 1. Premessa. – 2. Una nozione equivocata: l'ispezione informatica. – 3. La perquisizione informatica: caratteristiche generali. – 4. *Segue*: profili differenziali tra perquisizione disposta dall'autorità giudiziaria e perquisizione disposta dalla polizia giudiziaria. – 5. Il sequestro probatorio dei dati informatici: dal sequestro del "contenitore" al sequestro del "contenuto". – 6. *Segue*: le forme del sequestro. – 7. La copia dei dati, tra aspetti tecnici, ripetibilità ed irripetibilità dell'atto, rimedi impugnatori e necessità di individuazione codicistica di un relativo istituto autonomo. – 8. Profili peculiari in tema di richiesta di consegna ed esame presso banche di dati informatici. – 9. Le intercettazioni telematiche: le ragioni della disciplina ed il suo nucleo oggettivo. – 10. *Segue*: modalità captative, tra torsioni ed aporie sistematiche: a) il captatore informatico. – 11. *Segue*: b) il reindirizzamento.

1. *Premessa.*

Dopo avere considerato le caratteristiche generali che connotano le indagini informatiche occorre passare ad un'analisi più dettagliata dei singoli mezzi investigativi digitali.

Il continuo progresso tecnologico porta all'individuazione di nuove modulazioni e di inedite tipologie investigative sia sul fronte preventivo che repressivo e sia in riferimento agli atti d'indagine tipici che atipici, i quali vedono così ampliati i relativi cataloghi in un orizzonte in cui si delinea, però, anche una zona grigia, ove appare tutt'altro che agevole stabilire se un singolo atto sia ascrivile, sia pure in forza di una lettura

estensiva o evolutiva, ai mezzi tipici o se le caratteristiche che lo connotano lo sospingano oltre il perimetro degli atti nominati.

Occorre poi ricordare come, rispetto al tradizionale assetto investigativo, i mezzi di ricerca della prova informatici aprano brecce di più invasiva incidenza sul piano dei diritti fondamentali. Ne consegue che la loro ricostruzione interpretativa non può essere disgiunta dall'esigenza di individuare presidi adeguati, essendo anche consapevoli che, una volta ammesso l'impiego di un atto d'indagine, nella prassi è assai frequente che si tenda a dilatarne la sfera applicativa sia sul piano repressivo che preventivo.

Ciò premesso, l'attenzione si focalizzerà anzitutto sull'orizzonte repressivo, al cui interno verranno analizzate dapprima le indagini tipiche e, poi, quelle atipiche. In secondo luogo, ci si soffermerà sulle indagini preventive, nell'ottica delle interconnessioni che si delineano con il versante repressivo.

2. *Una nozione equivocata: l'ispezione informatica.*

Iniziando dalle indagini informatiche tipiche, si può ricordare come l'ispezione sia finalizzata ad «accertare le tracce e gli altri effetti materiali del reato»[1]. Dal canto suo, la perquisizione mira invece a reperire «il corpo del reato o cose pertinenti al reato»[2]. Il profilo differenziale tra i due mezzi di ricerca della prova viene dunque individuato nel fatto che l'ispezione assolve ad una funzione di osservazione e descrizione delle tracce e degli altri effetti materiali del reato, mentre la perquisizione ha come obiettivo la ricerca del corpo del reato e delle cose ad esso pertinenti.

In dottrina si è rilevato che l'ispezione è la «ricerca visiva di un segno»[3] e che «l'atto del perquisire differisce dall'ispezione nell'organo anatomico: mano e, rispettivamente, occhi; l'*inspiciens* scruta, il perquirente fruga»[4]. La linea di demarcazione tra i due istituti è, però, solo

---

[1] Cfr. art. 244 comma 1 c.p.p.

[2] Cfr. art. 247 c.p.p.

[3] Così F. CORDERO, *Procedura penale*, VIII ed., Giuffrè, Milano, 2006, p. 827.

[4] Così, F. CORDERO, *Procedura penale*, cit., p. 831.

apparentemente chiara. Ed il quadro legislativo non aiuta a definirla. Basti pensare a come l'art. 103 d.p.R. 9 ottobre 1990, n. 309 (*Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza*) preveda che la polizia giudiziaria possa «procedere in ogni luogo al controllo e all'ispezione dei mezzi di trasporto, dei bagagli e degli effetti personali» quando sussista il «fondato motivo di ritenere che possano essere *rinvenute* sostanze stupefacenti o psicotrope». Trattandosi di un'attività investigativa finalizzata al rinvenimento del corpo del reato, a rigore, essa sembrerebbe infatti qualificabile in termini di perquisizione. Dal canto suo, l'art. 27 legge 19 marzo 1990, n. 55 (*Nuove disposizioni per la prevenzione della delinquenza di tipo mafioso e di altre gravi forme di manifestazione di pericolosità sociale*) prevede la possibilità di procedere a «ispezione dei mezzi di trasporto, dei bagagli e degli effetti personali» quando vi sia «fondato motivo di ritenere che possono essere rinvenuti denaro o valori costituenti il prezzo della liberazione della persona sequestrata, o provenienti dai delitti predetti, nonché armi, munizioni o esplosivi». Anche se la previsione di una simile ispezione appare in linea con la sua configurazione sistematica e consente ad esempio di osservare l'abitacolo di un mezzo di trasporto, non bisogna dimenticare come la prassi applicativa abbia sovente fatto derivare dalla norma in esame la possibilità di effettuare un'attività non di ispezione, ma di vera e propria perquisizione.

Volendo comunque tenere ferma la distinzione tradizionale secondo la quale l'ispezione si esplica in un'attività di osservazione e la perquisizione in un'attività di ricerca, occorre chiedersi in che misura i due atti investigativi si possano declinare in riferimento alla realtà digitale.

Al riguardo, occorre anzitutto rilevare che mentre in riferimento alle perquisizioni la legge n. 48 del 2008 ha espressamente previsto la possibilità di superare eventuali misure di sicurezza poste a presidio dei sistemi informatici o telematici, nessuna analoga disposizione è stata dettata per le ispezioni. Circostanza che sembra confermare la mera funzione osservativa e descrittiva dell'ispezione, escludendo che essa possa consistere anche in attività materiali.

Dal canto suo, la prassi pare aver individuato come possibile oggetto di ispezione qualunque sistema o supporto informatico o telematico (*hardware* e *software* di *computer*, *hard disk*, *floppy-disk*, *cd-rom*, *usb-stick*, *dvd-rom*, *blue-ray*, telefoni cellulari, *smartphone*, *tablet*, *netbook*, *notebook*, navigatori satellitari, stampanti dotate di memoria, macchine fotografiche, lettori multimediali portatili, ecc.). Tuttavia, se qualunque attività sui dati o di controllo del contenuto di un dispositivo informatico sembra integrare più un'attività di ricerca che una mera attività di osservazione o di descrizione, riesce difficile concepire una ispezione prettamente informatica, se non nei limiti in cui sia funzionale ad un'osservazione esterna, che consenta di individuare ad esempio la marca del sistema informatico o la presenza di sistemi di connessione, quali rete *adsl* o rete *wireless*, nonché periferiche collegate o scollegate. In questo caso, però, a ben vedere, non si tratterebbe propriamente di un'attività informatica, ma di un'attività di osservazione *tout court*. Per questo motivo, ragionare in termini di ispezione informatica non appare convincente, dato che si rischia di confondere l'attività con l'oggetto della medesima. Sarebbe un po' come definire musicale un'ispezione solo perché ha ad oggetto uno strumento musicale.

In riferimento ai casi ed alle forme di perquisizione opportunamente, quindi, la legge n. 48 del 2008 non ha novellato l'art. 244 c.p.p. comma 1 – che disciplina l'ispezione di persone, luoghi e cose – ma soltanto il comma 2 del medesimo articolo, ammettendo in tale contesto la possibilità che i rilievi segnaletici, descrittivi e fotografici ed ogni altra operazione tecnica possano essere disposti dall'autorità giudiziaria anche in riferimento a sistemi informatici o telematici[5].

Al riguardo, occorre infatti rilevare come un conto siano i rilievi ispettivi e le operazioni tecniche disciplinate dall'art. 244 comma 2 c.p.p., altro conto le ispezioni *tout court* ai sensi dell'art. 244 comma 1 c.p.p. In particolare, i «rilievi tecnici» rappresentano attività volte ad acquisire «in via immediata e con elaborazione critica elementare dati della realtà, vale a dire materiale probatorio grezzo, destinato ad essere rielaborato in sede di indagini tecniche e peritali»[6]. Per un verso, tali

---

[5] Mediante l'adozione di «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Cfr. art. 244 comma 2 c.p.p. In argomento, cfr. G. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime*, Giuffrè, Milano, 2009, p. 193.

[6] Così R.E. KOSTORIS, *I consulenti tecnici nel processo penale*, Giuffrè, Milano,

rilievi possono certamente accedere ai mezzi tipici di ricerca della prova[7] e, quindi, anche all'ispezione, ma, per l'altro, essi rappresentano un'attività ben distinta da quella ispettiva. Le stesse considerazioni possono essere riferite anche alle operazioni tecniche, le quali, ancora una volta, rappresentano qualcosa che si aggiunge all'ispezione, ma che non coincide certo con essa.

Spetterà alla prassi individuare quali possano essere i rilievi ispettivi e le operazioni tecniche in materia, tenendo conto che il ricorso a tali atti investigativi non può certo rappresentare la modalità per eludere il presidio garantistico della disciplina degli accertamenti tecnici irripetibili che, come noto, prevede anche il diritto dell'indagato di nominare dei propri consulenti tecnici. Se così fosse, si verserebbe infatti in un'ipotesi di nullità di ordine generale a regime intermedio dell'atto investigativo ai sensi dell'art. 178 lett. c) c.p.p.[8].

Qualcuno riconduce ai rilievi ispettivi o alle operazioni tecniche la copia clone, anche se, come si vedrà (cfr. cap. IV, sez. I, § 7), varie ragioni inducono a ritenere che si tratti di un istituto diverso ed autonomo.

Appare invece più simile ad un'operazione tecnica la c.d. attività di *preview*. Si tratta di un atto investigativo che consente di vedere quanto contenuto in un sistema informatico mediante l'impiego di appositi *hardware* o *software*. Non sempre la *preview* è però idonea a garantire la non alterazione dei dati. A seconda dei casi essa si configura, infatti, come atto ripetibile o non ripetibile. In via generale, si può ritenere che integri un atto ripetibile quando venga effettuata a *computer* spento. Qualora il sistema fosse invece attivo o in *standby* il rischio di alterabilità dei dati sarebbe davvero elevato[9]. Del tutto residuali appaiono, poi,

1993, p. 141. In argomento, v., inoltre, D. CURTOTTI, *Rilievi e accertamenti tecnici*, Cedam, Padova, 2013.

[7] Cfr. R.E. KOSTORIS, *I consulenti tecnici nel processo penale*, cit., p. 143.

[8] Cfr. Cass., Sez. III, 11 ottobre 2012, n. 46715, secondo la quale, poi, sarebbe necessario dedurre una simile nullità non oltre la conclusione del giudizio di primo grado.

[9] In simili casi la *preview* potrebbe però «favorire l'identificazione di importanti informazioni che altrimenti non potrebbero essere rilevate (i processi attivi in quel determinato momento, i contenuti della memoria RAM, lo stato delle schede di rete, le tabelle di *routing*, ecc.)». G. COSTABILE (a cura di), *Nozioni ed elementi tecnici di principio*, in S. ATERNO-F. CAJANI-G. COSTABILE-M. MATTIUCCI-G. MAZZARACO, Computer forensics *e indagini digitali, Manuale tecnico-giuridico e casi pratici*, vol. I, Experta, Forlì, 2011, vol. I, p. 21. In argomento, cfr. anche P. FELICIONI, *Ispezioni*, in P. FERRUA-E. MARZADURI-G. SPANGHER (a cura di), *La prova penale*, Giappichelli, Torino, 2013, p. 668, n. 191.

le ipotesi in cui la *preview* rappresenti un atto ripetibile in rapporto ai telefoni cellulari. Tra esse si può comunque ricordare il caso in cui venga effettuata sulle c.d. schede aggiuntive di memoria di un cellulare rinvenuto spento.

Quanto alla sua qualificazione giuridica, occorre precisare come la *preview* permetta non solo di vedere, ma anche di ricercare. Per questo motivo, in dottrina è stato proposto di qualificare in termini di ispezione la fase osservativa, mentre come perquisizione quella di ricerca di eventuali *file*, testi o immagini[10]. In questa prospettiva, la *preview* risulterebbe quindi un atto investigativo complesso composto per un verso da un'indagine ispettiva e per l'altro da una perquisizione. Una simile impostazione non appare però del tutto convincente, dato che sul piano operativo i due momenti finiscono spesso per sovrapporsi rendendosi di fatto indistinguibili.

Dal che si può trarre ulteriore conferma di come l'ispezione sia un istituto che mal si adatta alle indagini informatiche.

3. *La perquisizione informatica: caratteristiche generali.*

Dal canto suo, la perquisizione è un atto a sorpresa tipico che mira alla ricerca del corpo del reato o delle cose ad esso pertinenti o, ancora, all'arresto dell'imputato o dell'evaso. Analogamente all'ispezione, anche questo mezzo di ricerca della prova è stato concepito per contesti caratterizzati dalla materialità delle cose su cui insiste l'atto investigativo. In questa prospettiva, il codice del 1988 aveva individuato due possibili forme di perquisizione: la perquisizione personale e quella locale.

Tuttavia, poiché in un'era sempre più tecnologica, nell'orizzonte di-

[10] Cfr. S. ATERNO, *Commento all'art. 8: Modifiche al titolo III del libro III del codice di procedura penale*, in G. CORASANITI-G. CORRIAS LUCENTE (a cura di), Cybercrime, *responsabilità degli enti, prova digitale*, Cedam, Padova, 2008, p. 206 s.

gitale si conserva ampia traccia delle vite di ciascuno, *computer*, *tablet*, telefoni cellulari, *Cloud* e, in generale, sistemi informatici possono custodire elementi di prova, talora determinanti ai fini investigativi. Inevitabile, quindi, che si ponga la necessità di effettuare delle ricerche all'interno di questi "luoghi informatici".

Consapevole di ciò, il legislatore della legge n. 48 del 2008 ha rimodulato la disciplina delle perquisizioni per adattarla alla nuova realtà tecnologica. E lo ha fatto mediante due innesti normativi.

Anzitutto, in riferimento alla disciplina prevista per i casi e le forme di perquisizione ha aggiunto all'art. 247 c.p.p. un comma 1-*bis*, secondo il quale quando «vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

In secondo luogo, ha previsto nell'ambito delle attività a iniziativa della polizia giudiziaria l'inserimento di un comma 1-*bis* nell'art. 352 c.p.p. in forza del quale, nella flagranza del reato, in caso di evasione, ovvero qualora si debba procedere alla esecuzione di un'ordinanza che prevede la custodia cautelare o di un ordine che dispone la carcerazione nei riguardi di una persona imputata o condannata per uno dei delitti previsti all'art. 380 c.p.p.[11] o, ancora, al fermo di indiziato di delitto, se sussistono particolari motivi di urgenza che non permettono di attendere l'emissione del decreto di perquisizione «gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi».

Tale perquisizione informatica non deve però essere confusa con la c.d. perquisizione *on line*, così denominata per talune somiglianze che presenta con l'istituto della perquisizione, ma dal quale si distingue per specifiche peculiarità e per l'impossibilità di riferire ad essa le garanzie

[11] Si tratta dei delitti che legittimano l'arresto obbligatorio in flagranza.

previste per le perquisizioni. Di essa si tratterà nella sezione seconda del capitolo[12], mentre in questa sede ci si concentrerà sulla perquisizione informatica in senso proprio.

Al riguardo, sembra opportuno chiedersi se quest'ultima sia riconducibile ad una mera declinazione della perquisizione ordinaria o se la stessa integri invece un'autonoma tipologia di perquisizione. La parziale diversità e modulazione dei diritti fondamentali lesi, la diversità dei presupposti che la legittimano, le peculiari caratteristiche dell'oggetto su cui insiste, nonché le specifiche modalità con cui deve essere effettuata inducono a ritenere che la perquisizione di un sistema informatico o telematico configuri una nuova tipologia di perquisizione. Sembra quindi possibile concludere che, a seguito dell'entrata in vigore della legge n. 48 del 2008, il codice di rito contempli tre forme di perquisizione: locale, personale ed informatica.

Naturalmente, al pari di ogni perquisizione, anche quest'ultima è subordinata all'esistenza di una *notitia criminis*, non essendo certo consentita la rievocazione di una sorta di *inquisitio generalis*[13] attraverso il monitoraggio preventivo, continuo e permanente di un sistema informatico[14]. Inoltre, affinché «non vengano pregiudicate le garanzie difensive e i diritti costituzionalmente protetti dagli artt. 14 e 15 Cost. (...) le perquisizioni informatiche devono essere "mirate"»[15].

Si può infine ricordare una particolare ipotesi di perquisizione, dato che essa rende evidente la necessità di ampliare la nozione di "luogo" oggetto dell'attività perquirente includendovi anche il *computer* ed il

[12] Cfr. cap. IV, sez. II, § 8.

[13] Cfr. F. CORDERO, *Criminalia. Nascita dei sistemi penali*, Lampi di stampa, Milano, 1999, p. 664, nonché R. ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*Inquisitio generalis, cit., p. 568 ss. Per una riflessione sull'«atto della scoperta» del reato si rinvia a E. FRAGASSO JR., *L'atto della scoperta tra diritto e logica*, in *Arch. pen.*, *I libri*, 2012, p. 81 ss.

[14] In questo senso, in riferimento alla perquisizione ed al sequestro volti a identificare preventivamente i passeggeri presunti corrieri internazionali di stupefacenti, cfr. Cass., Sez. IV, 17 aprile 2012, n. 19618. In argomento, cfr. G. BONO, *Il divieto di indagini ad explorandum include i mezzi informatici di ricerca della prova*, in *Cass. pen.*, 2013, p. 1525 ss.

[15] Così, S. LORUSSO, *Sequestro probatorio e tutela del segreto giornalistico*, in *Giur. it.*, 2015, p. 1505.

Cloud. Ci si riferisce alle perquisizioni di sistemi informatici o telematici utilizzati da un difensore.

È noto come l'art. 103 c.p.p. preveda che le perquisizioni ordinarie presso gli uffici del difensore si svolgano con il rispetto di particolare garanzie. Si deve però rilevare come l'impiego dei moderni strumenti tecnologici renda meno chiara l'individuazione del concetto di «ufficio del difensore». Quest'ultimo rimane indubbiamente un luogo fisico definito, ma è anche vero che i dati attinenti all'attività difensiva possono trovarsi pure in *tablet*, *pc* portatili, cellulari di ultima generazione, che spesso rappresentano strumenti dall'impiego molteplice, potendo essere utilizzati sia a scopo personale sia ai fini di un'attività difensiva. Se la *ratio* della disciplina prevista all'art. 103 c.p.p. è rappresentata dalla tutela del diritto di difesa, un simile diritto pare dover essere tutelato anche quando si proceda ad una perquisizione su sistemi informatici o telematici usati a fini professionali dal difensore, a prescindere dal fatto che essi si trovino concretamente ubicati presso un ufficio, rilevando il fatto che essi rappresentino un "luogo di lavoro". Ne deriva che una perquisizione in tali "luoghi informatici" appare legittima solo se svolta nel rispetto delle previste garanzie, che si esplicano nel previo avviso da parte dell'autorità giudiziaria al consiglio dell'ordine forense [16] e nella circostanza che il giudice provveda personalmente alla perquisizione, a meno di non autorizzare con decreto motivato il pubblico ministero a svolgerla.

Si tratta di garanzie che sembrano venire meno nella sola ipotesi in cui l'indagato sia il difensore stesso [17]. Diversamente opinando, infatti, si verificherebbe un allargamento della tutela della persona sottoposta alle indagini al di fuori della *ratio* della norma. Nel caso in cui sia indagato il difensore il potere di disporre una perquisizione su sistemi informatici o telematici nell'ambito di un procedimento penale spetterebbe di conseguenza al pubblico ministero e non al giudice per le indagini preliminari.

[16] Ai sensi dell'art. 103 comma 3 c.p.p. tale avviso è previsto a pena di nullità.

[17] Cfr. Cass, Sez. III, 7 giugno 2017, n. 28069. In dottrina, cfr. A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè, Milano, 1996, p. 132.

4. Segue: *profili differenziali tra perquisizione disposta dall'autorità giudiziaria e perquisizione disposta dalla polizia giudiziaria.*

Le perquisizioni informatiche possono essere disposte dalla autorità giudiziaria o dalla polizia giudiziaria. Quanto alla prima locuzione, come è noto, essa è idonea a ricomprendere anche il pubblico ministero [18]. In materia, poi, non è prevista la convalida dell'atto da parte del giudice per le indagini preliminari. Si tratta di una scelta convincente, dato che una generalizzazione dell'intervento giurisdizionale in rapporto ai mezzi di ricerca della prova sembrerebbe trasformare il giudice per le indagini preliminari in magistrato istruttore [19].

La disciplina delle perquisizioni informatiche presenta aspetti talora comuni, talora diversi a seconda che sia disposta dall'autorità giudiziaria o dalla polizia giudiziaria.

Un profilo che differenzia le due forme di perquisizioni è rappresentato anzitutto dai presupposti che le legittimano. Quella disposta dalla polizia giudiziaria presuppone la flagranza di un reato, o la necessità di procedere alla esecuzione di un'ordinanza che dispone la custodia cautelare o di un ordine che dispone la carcerazione nei confronti di una persona imputata o condannata per uno dei delitti previsti dall'art. 380 c.p.p., o, ancora, il fermo di una persona indiziata di delitto, in presenza di particolari motivi di urgenza che non consentono la emissione di un tempestivo decreto di perquisizione da parte dell'autorità giudiziaria. Nel complesso si tratta di requisiti che fanno leva sull'urgenza di agire e che non figurano in rapporto alla perquisizione disposta dall'autorità giudiziaria.

Tra gli aspetti comuni alle due tipologie di perquisizione figura invece la presenza del «fondato motivo» di ritenere [20] che elementi digitali pertinenti al reato si trovino in un sistema informatico. Si tratta di un requisito che non caratterizza le sole perquisizioni informatiche, ma le

[18] Al riguardo, cfr. M. BARGIS, voce *Perquisizione*, in *Dig. disc. pen.*, vol. IX, Utet, 1995, p. 501.

[19] In proposito, cfr. P. FELICIONI, *Le ispezioni e le perquisizioni*, Giuffrè, Milano, 2004, p. 47.

[20] Si può ricordare come l'art. 332 comma 1 c.p.p. abr. legittimasse invece perquisizioni basate sul solo sospetto.

perquisizioni in generale, in riferimento alle quali il «fondato motivo» è stato considerato integrato ora da un plausibile sospetto, ora da un *quid pluris* rappresentato da concreti indizi, ora dall'esistenza di elementi obiettivi che inducano a ritenere che una cosa si trovi in un determinato luogo sulla scorta di un ragionamento probabilistico. In definitiva, esso esprime un concetto che esclude semplici congetture, dovendosi ancorare alla necessaria esistenza di elementi oggettivi.

Nel caso della perquisizione informatica di iniziativa della polizia giudiziaria, il concetto di «fondato motivo» viene poi specificato, nel senso che esso deve consentire di ritenere che in un sistema informatico o telematico si «trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi». Per contro, nel caso di perquisizione informatica disposta dall'autorità giudiziaria, deve sussistere solo un fondato motivo di ritenere che «dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico». Le differenze che intercorrono tra le due ipotesi in ordine al «fondato motivo» sembrano essere due. L'una solo apparente, l'altra effettiva.

La prima riguarda la diversa espressione impiegata per definire la modalità di "ubicazione" degli elementi di prova: infatti, per le perquisizioni di iniziativa della polizia giudiziaria si prevede che tali elementi di prova «si trovino *occultati*»; per quelle disposte dall'autorità giudiziaria è invece sufficiente che i medesimi «si trovino» in un sistema informatico o telematico. In realtà, nonostante il riferimento all'occultamento compaia di rado nel codice di rito, esso appare pleonastico nell'ambito della disciplina delle perquisizioni. Non sembra infatti che esso alluda ad un *quid pluris* rispetto al mero fatto che i dati «si trovino» in un sistema informatico o telematico. Diversamente, si giungerebbe ad un'interpretazione del tutto fuorviante, in quanto porterebbe a ritenere ammissibile la perquisizione di iniziativa della polizia giudiziaria solo quando occorra ricercare qualcosa che non solo si trovi all'interno di un sistema informatico o telematico, ma risulti in esso celato, come nell'ipotesi di ricerca di *file* cancellati oppure di dati nascosti in altri *file*, ad esempio mediante l'uso di una tecnica denominata steganografia, o di dati protetti da misure di sicurezza, restringendo in tal modo inopinatamente i poteri della polizia giudiziaria.

Venendo invece, in rapporto al requisito del «fondato motivo», alla

differenza effettiva che intercorre tra le perquisizioni di iniziativa della polizia giudiziaria e quelle disposte dall'autorità giudiziaria, occorre rilevare come solo per le prime si richieda il fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato possano «essere cancellati o dispersi». Viene, quindi, posto l'accento sul *periculum in mora*, rappresentato dall'esposizione al rischio della cancellazione o dispersione. Si tratta di un presupposto che il legislatore ha mutuato dalla disciplina in tema di perquisizioni personali e locali prevista dall'art. 352 comma 1 c.p.p. e che indica chiaramente come la polizia giudiziaria possa effettuare perquisizioni informatiche di propria iniziativa soltanto in caso di urgenza. È peraltro vero che date le caratteristiche che connotano i dati digitali (volatilità, facile alterabilità e modificabilità), il pericolo di cancellazione o dispersione appare quasi *in re ipsa*, almeno in tutti i casi in cui il dispositivo informatico sottoposto a perquisizione venga rinvenuto acceso. Esistono, infatti, dati che potrebbero andare irrimediabilmente perduti nel caso in cui l'atto investigativo venisse procrastinato[21].

Le perquisizioni informatiche disposte dall'autorità giudiziaria e dalla polizia giudiziaria presentano poi ulteriori tratti comuni. Anzitutto, rispetto ad entrambe si prevede la possibilità di effettuare la perquisizione anche quando il sistema risulti protetto da misure di sicurezza e in rapporto ad entrambe si richiede che i perquirenti adottino «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Quest'ultima prescrizione appare quanto mai opportuna, dato che nella prassi si erano registrate delle devianze applicative che avevano determinato addirittura l'alterazione o l'eliminazione involontaria di elementi di prova digitali. Tuttavia, la norma non sembra tenere conto che, allo stato della tecnica, in taluni casi risulta impossibile adottare misure tecniche volte a preservare la genuinità dei dati. Si pensi ad esempio al caso di flagranza del reato di spaccio di sostanza stupefacente. In simili ipotesi l'immediata perquisizione del cellulare dell'arrestato può risultare di estrema utilità per ricostruire la rete

[21] A titolo esemplificativo, si possono ricordare i *file* temporanei, *cache* di sistema, pagine *web*, *mail* in bozza, conversazioni in *chat*. Al riguardo, cfr. D. BUSO-D. PISTOLESI, *Le perquisizioni e i sequestri informatici*, in F. RUGGIERI-L. PICOTTI (a cura di), cit., p. 189.

dei contatti e dei possibili accordi di cessioni di sostanza. L'urgenza di una tale perquisizione è però incompatibile con l'adozione di misure tecniche volte alla conservazione della genuinità dei dati. Tuttavia, non è affatto detto che i dati potenzialmente alterabili siano necessariamente i dati rilevanti per le indagini.

In definitiva, l'osservanza delle misure tecniche volte ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione rappresenta in via di principio un'ineludibile necessità per garantire la genuinità della fonte di prova e deve rappresentare la regola a cui conformare le investigazioni. Tuttavia, la sua osservanza non può prescindere comunque da un rapporto di finalizzazione rispetto all'attività di indagine, dovendosi di volta in volta verificare se i dati di cui non è possibile preservare la genuinità siano davvero rilevanti per le indagini in rapporto al caso concreto.

5. *Il sequestro probatorio dei dati informatici: dal sequestro del "contenitore" al sequestro del "contenuto".*

Il sequestro probatorio è funzionale ad assicurare al procedimento una cosa mobile o immobile, necessaria all'accertamento dei fatti. Esso implica la privazione del possesso della cosa e crea sulla stessa un vincolo di indisponibilità.

L'oggetto su cui insiste è inoltre rappresentato dal corpo del reato e dalle cose pertinenti al reato. Nell'impostazione tradizionale, simili oggetti presentano la caratteristica comune di essere materiali.

Quanto al corpo del reato, il suo stesso *nomen iuris*[22] sembra rinviare ontologicamente al concetto di materia, appartenendo alla «fisica del reato»[23]. Tuttavia, l'avvento del digitale ha reso possibile individuare

[22] Tradizionalmente, la nozione di corpo di reato si compone di due elementi: materialità e rapporto di relazione tra cosa e reato. Cfr. C.U. DEL POZZO, voce *Corpo del reato*, in *Enc. dir.*, vol. X, Giuffrè, Milano, p. 650, nonché S. RUGGERI-P. MAGGIO, *Il sequestro probatorio*, in P. FERRUA-E. MARZADURI-G. SPANGHER (a cura di), *La prova penale*, Giappichelli, Torino, 2013, p. 785.

[23] Così, F. CORDERO, *Procedura penale*, VIII ed., Giuffrè, Milano, p. 841.

anche corpi del reato immateriali. Si pensi ad una diffamazione *on line*, commessa attraverso l'inoltro di una *e-mail* a più persone. Difficile ritenere che quest'ultima non rappresenti il corpo del reato e che non sia qualificabile in termini di "cosa" tale da integrare il presupposto previsto dall'art. 253 comma 2 c.p.p., secondo il quale sono corpo del reato le cose sulle quali o mediante le quali il reato è stato commesso.

Dal canto suo, anche la nozione di «cosa pertinente al reato»[24] è stata inizialmente intesa in senso fisico naturalistico[25], per essere poi dilatata fino a ricomprendere anche i dati digitali.

Invero, sia in riferimento al corpo del reato che alla cosa pertinente al reato si può ricordare come prima della legge n. 48 del 2008 si fosse dubitato della possibilità di sequestrare, nell'ambito di un'attività investigativa, i dati contenuti in un *computer*, in uno *smartphone*, o in qualsiasi altro sistema informatico a prescindere dal sequestro del supporto che li conteneva poiché appariva assai dubbia la possibilità di qualificare simili dati alla stregua di elementi materiali[26] e, quindi, di "cose". Di fronte alla mancanza di una corporeità visibile degli elementi di prova digitali, la dottrina processualpenalistica aveva inizialmente avvertito un certo disagio nel configurare elementi probatori o prove disgiunte dal requisito della fisicità[27]. Di qui l'equivoco di fondo, che in passato ave-

[24] Per un'analisi della fluidità di un simile concetto, cfr. C. GABRIELLI, *Il sequestro probatorio non supera il riesame: la copia dell'*hard disk *ritorna al giornalista, sia pure con qualche "scorciatoia" argomentativa*, in *Giur. di mer.*, f. 4, 2007, p. 200 ss.

[25] Si può ricordare come anche sul piano del diritto penale sostanziale ci si fosse a lungo interrogati sulla possibilità di riferire il concetto di «cosa» a realtà immateriali. Una simile riflessione aveva ad esempio indotto il legislatore a specificare in tema di reato di esercizio arbitrario delle proprie ragioni (art. 392 comma 3 c.p.) che la violenza sulle cose si può realizzare anche quando viene «alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico», lasciando così intendere che non fosse in precedenza chiaro se questi ultimi potessero ritenersi già ricompresi nella nozione di "cosa".

[26] Certo, da un punto di vista fisico, ad essi corrisponde una fisicità, essendo costituiti da impulsi elettrici e rappresentando quindi una "materia", che poi si traduce in una sequenza numerica di "zero e uno". Al riguardo, cfr. S. ATERNO, *La* computer forensic *tra teoria e prassi: elaborazioni dottrinali e strategie processuali*, in *Ciberspazio e diritto*, 4/2006, p. 427.

[27] Per una riflessione sulle conseguenze di tale difficoltà, cfr. M. DANIELE, *Caratte-*

va portato ad identificare gli elementi di prova digitali con il supporto nel quale essi erano memorizzati. In questa prospettiva, sembra dover essere considerata anche l'emissione di decreti di sequestro che avevano ad oggetto l'intero *computer*, o addirittura i *mouse*, i relativi tappetini, le casse acustiche e i cavi elettrici[28], secondo un orientamento, che era stato avallato anche dalla Corte di Cassazione, la quale riteneva che tra questi ultimi e i dati informatici sussistesse un "vincolo pertinenziale"[29].

Solo in un secondo momento, quindi, è maturata la consapevolezza che i dati, le informazioni, i programmi possono di per sé integrare i concetti di «corpo del reato» o di «cosa pertinente al reato» e che, ai fini del sequestro, è spesso sufficiente disporre dei dati e non anche del *computer* o del sistema informatico che li contiene[30]. Ciò anche nell'ottica che dal provvedimento di sequestro derivi la minore afflittività possibile[31] e che tale atto sia ispirato al canone di proporzionalità.

---

ristiche della prova digitale, in F. RUGGIERI-L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Giappichelli, Torino, 2011, p. 204.

[28] Al riguardo, cfr. Trib. Riesame Potenza, ord. 2 maggio 2002, p.p. n. 132/02 R.G.; Trib. Riesame Salerno, ord. 5 ottobre 2002, p.p. n. 6848/02 R.G.; Trib. Riesame Roma, ord. 24 dicembre 2002, p.p. 3589/02 R.G.; Trib. Riesame Venezia, ord. 31 maggio 2005, p.p. 2082/05 R.G.; Trib. Riesame Perugia, ord. 25 ottobre 2006, p.p. n. 7033/06 R.G. Tali sentenze, a quanto ci consta inedite, sono richiamate da A. MONTI, *La nuova disciplina del sequestro informatico*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime, Giuffrè, Milano, 2009, p. 199, n. 10. V., inoltre, F. BRAVO, *Indagini informatiche e acquisizione della prova nel processo penale*, in *Riv. crim., vitt. e sicur.*, sett. 2009-apr. 2010, p. 237.

[29] Cfr. Cass. 3 aprile 2008, n. 13792.

[30] Si vedano i rilievi di G. VACIAGO, *Le investigazioni telematiche*, in M.L. PICCININI-G. VACIAGO, *Computer crime. Casi pratici e metodologie investigative dei reati informatici*, Moretti Honegger, Bergamo, 2008, p. 102, nonché di A.C. MANCHIA, *Sequestro di computers: un provvedimento superato dalla tecnologia?*, in *Cass. pen.*, 2005, p. 1634 ss. Sotto altro profilo occorre ricordare come sia ormai acquisita la consapevolezza che i dati digitali sussistono a prescindere dal supporto su cui sono assicurati. Sul punto, v. L. PICOTTI, *La ratifica della Convenzione cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, p. 702 s.

[31] Cfr. A. MONTI, *La nuova disciplina del sequestro informatico*, in L. LUPARIA (a cura di), *Sistema penale e criminalità informatica*, cit., p. 199. Sulla problematica dell'esperibilità del riesame avverso il decreto di sequestro probatorio quando l'oggetto

È in questa prospettiva che la legge n. 48 del 2008 ha disciplinato la possibilità di sequestro di dati informatici, chiarendo anche che le *e-mail* e le forme similari di comunicazione rappresentano a tutti gli effetti una forma di "corrispondenza"[32] suscettibile di sequestro ai sensi dell'art. 254 c.p.p. Tale legge non ha poi mancato di introdurre l'art. 254-*bis* c.p.p., specificamente dedicato ai sequestri di dati informatici[33] presso fornitori di sevizi informatici, telematici e di telecomunicazioni.

6. Segue: *le forme del sequestro.*

Sul piano operativo, il sequestro sembra poter essere effettuato soltanto in due forme, affatto fungibili. Da un lato, attraverso il c.d. "blocco dei dati"; dall'altro, mediante il sequestro dell'intero dispositivo informatico.

Il primo, si traduce in un'operazione tecnica volta a "congelare" i dati presenti in un dispositivo informatico, che vengono anche "sigillati" elettronicamente, in modo da garantirne l'intangibilità e la non alterabilità. Il "blocco dei dati" non deve essere confuso con il c.d. *freezing* degli stessi. Quest'ultimo non è un atto ablativo e non sembra affatto rappresentare una forma di sequestro. Disciplinato dall'art. 132 commi 4-*ter*, 4-*quater* e 4-*quinquies* codice *privacy* esso corrisponde infatti ad una particolare modalità di conservazione e protezione dei dati per un periodo non superiore a novanta giorni che può essere effettuata dai fornitori e dagli operatori di servizi informatici o telematici a fini preventivi e repressivi[34].

---

di tale mezzo di ricerca della prova venga riconsegnato al detentore, previa riproduzione del suo contenuto, cfr. S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, cit., p. 472 ss., nonché G. TODARO, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare:* revirement *delle Sezioni Unite*, in *Dir. pen. cont.*, n. 11, 2017, p. 157 ss. In giurisprudenza, cfr. Cass., Sez. Un., 24 aprile 2008, n. 18253, nonché Id. 7 settembre 2017, n. 40963.

[32] In tema di sequestro di corrispondenza, l'art. 254 c.p.p. fa infatti riferimento ad «altri oggetti di corrispondenza, anche se inoltrati per via telematica».

[33] Sottolinea la necessità di non accedere ad interpretazioni estensive della norma A. MACRILLÒ, *Le nuove disposizioni in tema di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. dell'internet*, 2008, p. 514.

[34] In tema, cfr. C. MAIOLI-E. SANGUEDOLCE, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, in *Altalex*, 7 maggio 2012.

Venendo al sequestro dell'intero dispositivo informatico, occorre rilevare come esso miri all'apprensione dei dati contenuti in tale dispositivo[35]. Si tratta di un provvedimento ablativo che deve configurarsi come proporzionato[36] rispetto alle esigenze di accertamento dei fatti oggetto delle indagini, risultando di regola meno invasivo il diverso atto di copia dei dati. La valutazione della proporzionalità del sequestro dovrà poi accompagnarsi anche alla verifica che lo stesso non divenga strumentale all'aggiramento delle garanzie, come accadrebbe se esso fosse finalizzato a conoscere in modo «incontrollato» la fonte delle informazioni di un giornalista[37], con elusione delle discipline previste dagli artt. 200 comma 3 c.p.p. e 256 c.p.p.[38].

Ciò premesso, sembra opportuno porre in rilievo un ulteriore aspetto che caratterizza sia il sequestro effettuato mediante blocco di dati, sia quello del dispositivo informatico. Mentre nelle indagini tradizionali la perquisizione precede di regola il sequestro, nel caso delle investigazioni informatiche è frequente che un simile rapporto si inverta, nel senso che si sequestra un dispositivo informatico per procedere poi a perquisizione.

Dal fatto che il sequestro del dispositivo può precedere la perquisi-

[35] In argomento, v. G. ILLUMINATI, *Le direttive del d.d.l. n. 4368*, in *JusOnline*, 3/2017, p. 329.

[36] Per l'applicabilità di tale principio anche in rapporto ai vincoli di natura reale, cfr., *ex multis*, Cass., Sez. III, 16 maggio 2012, n. 21931, nonché Id., Sez. III, 7 maggio 2014, n. 21271.

[37] In argomento, cfr. S. LORUSSO, *Sequestro probatorio e tutela del segreto giornalistico*, cit., p. 1503 ss. Dal canto suo, la Corte di Strasburgo non ha mancato di rimarcare che la libertà di espressione rappresenta uno dei fondamenti su cui regge la stessa società democratica, con la conseguente necessità di accordare particolare garanzie alla stampa. Cfr. Corte eur., Grande Camera, 14 settembre 2010, *Sanoma Uitgevers B.V. c. Paesi Bassi*, nonché Corte eur., sez. V, 20 marzo 2012, *Martin e altro c. Francia*, 2012, in *Cass. pen.*, n. 11, p. 3910. In dottrina, cfr. inoltre M. CASTELLANETA, *La libertà di stampa nel diritto internazionale ed europeo*, Cacucci, Bari, 2012. Si può ricordare che in tema di doveri di esibizione e segreti l'art. 256 c.p.p. prevede che le persone indicate negli artt. 200 e 201 c.p.p. debbano consegnare immediatamente all'autorità giudiziaria che li richieda dati, informazioni, programmi informatici, *anche mediante copia* di essi da assicurare su un idoneo supporto.

[38] Cfr. Cass. pen., Sez. VI, 18 luglio 2014, n. 31735, nonché Id., Sez. VI, 10 giugno 2015, n. 24617.

zione informatica sembrano poter derivare delle conseguenze sistematiche in rapporto alle indagini tradizionali. In particolare, tale profilo pare rappresentare un indice *a contrario* rispetto all'impostazione secondo la quale tra perquisizione e sequestro sussisterebbe un nesso sinergico-funzionale di logica consequenzialità. È noto come, muovendo da questo presupposto ed adattando all'ipotesi in esame la teoria «dei frutti dell'albero avvelenato», dalla illegittimità della perquisizione venga fatta derivare l'illegittimità del successivo sequestro[39]. Opzione interpretativa solo in parte mitigata dalle Sezioni Unite, le quali, dopo aver ribadito che la perquisizione illegittima riverbera i propri effetti invalidanti anche sul sequestro, hanno però sottolineato che una simile conseguenza non si verifica nell'ipotesi di sequestro del corpo del reato o delle cose pertinenti al reato, dato che tale sequestro si configurerebbe come un «atto dovuto», la cui omissione «esporrebbe gli autori a specifiche responsabilità penali, quali che siano state, in concreto, le modalità propedeutiche e funzionali che hanno consentito l'esito positivo della ricerca compiuta»[40].

Tuttavia, proprio il fatto che nel quadro delle indagini digitali il sequestro possa precedere la perquisizione aiuta a comprendere che la propedeuticità della seconda rispetto al primo rappresenta al più un mero dato di frequenza statistica e non una necessità logico giuridica. Inoltre, il sequestro è spesso funzionale a consentire la copia dei dati, sulla quale verrà poi effettuata la perquisizione. Ne consegue che perquisizione e sequestro sembrano integrare due mezzi di ricerca della prova autonomi. Sicché non sembra individuabile alcun effetto a cascata per il quale l'illegittimità della perquisizione determini di per sé l'illegittimità del successivo sequestro. In definitiva, la legittimità di quest'ultimo andrà valutata atomisticamente alla luce della mera sussistenza

[39] In argomento, cfr. L.P. COMOGLIO, *Perquisizione illegittima ed inutilizzabilità derivata delle prove acquisite con il susseguente sequestro*, in *Cass. pen.*, 1996, p. 1547 ss.; M. NOBILI, *Divieti probatori e sanzioni*, in *Giust. pen.*,1991, III, c. 641; A. ZAPPULLA, *Le indagini per la formazione della* notitia criminis: *il caso della perquisizione seguita da sequestro*, in *Cass. pen.*, 1996, p. 1878 ss.

[40] Così, Cass., Sez. Un., 27 marzo 1996, S., in *Cass. pen.*, 1996, p. 3273. Sulla stessa linea, Cass., sez. III, 17 febbraio 2016, n. 19365; Id., Sez. II, 23 dicembre 2016, n. 15784. In dottrina, cfr. E. FORTUNA-S. DRAGONE, *Le prove*, in E. FORTUNA-S. DRAGONE-E. FASSONE-R. GIUSTOZZI, *Manuale pratico del processo penale*, Cedam, Padova, 2007, p. 400.

dei requisiti che lo legittimano e non come derivata da una perquisizione illegittima.

7. *La copia dei dati, tra aspetti tecnici, ripetibilità ed irripetibilità dell'atto, rimedi impugnatori e necessità di individuazione codicistica di un relativo istituto autonomo.*

La finalità di apprendere i dati digitali contenuti in un dispositivo o in un sistema informatico può essere raggiunta anche mediante la copia dei dati[41], la quale viene spesso considerata una forma privilegiata di sequestro informatico[42]. In prosieguo, si tenterà invece di dimostrare come tale copia non sembri integrare una modalità di sequestro, ma piuttosto un autonomo atto investigativo. A tal fine pare opportuno chiarire però, preliminarmente, le caratteristiche tecniche della copia. Su questa base, si verificherà se un simile atto si configuri come ripetibile o irripetibile. Infine ci si concentrerà sul suo possibile inquadramento sistematico e sulla possibilità di esperire il riesame per la restituzione della copia.

a) Da un punto di vista tecnico la copia dei dati può essere effettuata in due modi.

Anzitutto, mediante la c.d. riproduzione logica, che attua però una duplicazione imperfetta, omettendo di copiare taluni dati, come i c.d. dati non allocati.

La seconda modalità di copia è invece del tutto identica all'originale. È una copia *bit a bit*, che finisce per trascendere la sua stessa natura, divenendo un secondo originale. In particolare, al fine di garantire la genuinità dei dati, gli investigatori sono soliti ricorrere preliminarmente al c.d. *Write Blocker*, il quale rappresenta una tecnica idonea ad impedire la loro modifica. Successivamente è possibile creare la c.d. *bit stream image*, ossia la copia, che si caratterizza per la capacità di svolgere la

[41] In argomento, cfr. S. FASOLIN, *La copia di dati informatici nel quadro delle categorie processuali*, in *Dir. pen. proc.*, 2012, p. 372 ss.

[42] Tra coloro che qualificano la copia dei dati alla stregua di una forma di sequestro, cfr., *ex multis*, M. PITTIRUTI, Digital evidence *e procedimento penale*, Giappichelli, Torino, 2017, p. 38.

c.d. operazione di *hashing*. Si tratta di un algoritmo che consente di trasformare il dato oggetto di copia in una stringa alfanumerica[43], la quale costituisce una sorta di "impronta digitale" del dato, permettendo di verificare in ogni momento che il contenuto della copia sia conforme all'originale. Infatti, qualora mutasse anche un solo *bit*, il sistema elaborerebbe una diversa stringa alfanumerica. La creazione della *beat stream image* avviene mediante l'impiego dei c.d. *tool*[44], vale a dire di appositi programmi informatici[45], che consentono di cristallizzare i dati informatici senza che gli stessi subiscano alterazioni. È stato rilevato che i *tool* impiegati per realizzare le copie clone sono di regola programmi commercializzati da società e coperti da licenza, con la conseguenza che, al di là della società proprietaria, nessuno è in grado di conoscere i c.d. codici sorgente. Alla luce di ciò, è stato poi sottolineato che le parti potrebbero sostenere l'impossibilità sia di verificare il funzionamento del *software*, sia di analizzare il percorso da esso seguito, sia, in ultima analisi, di accertare che la copia sia davvero conforme all'originale[46]. Una simile impostazione non appare però convincente. Gli stessi tradizionali programmi (si pensi a *Windows*) si basano su codici sorgenti non conosciuti, ma non si dubita per questo della loro idoneità rappresentativa[47].

[43] La lunghezza dei valori di *hash* non è costante, ma varia in relazione al tipo di algoritmo utilizzato. I tecnici del settore consigliano peraltro di utilizzare in ambito investigativo algoritmi, qual è SHA, che consentano di fornire *hash* di 224, 256, 348 e 512 *bit*. Cfr. G. COSTABILE, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Ciberspazio e dir.*, 2010, p. 500.

[44] Sulla problematica dei *tool* e sulle procedure dell'investigatore informatico, v. G. ZICCARDI, *Aspetti informatico-giuridici della fonte di prova digitale*, in L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, Milano, 2007, p. 55.

[45] Al riguardo, cfr. F. NOVARIO, *Le prove informatiche*, in P. FERRUA, E. MARZADURI-G. SPANGHER (a cura di), *La prova penale*, cit., p. 124 ss. nonché G. ZICCARDI, *Aspetti informatico-giuridici della fonte di prova digitale*, in L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, Milano, 2007, p. 55. Tra i *tool* di frequente impiego da parte delle forze di polizia europee e americane può essere ricordato *Encase*.

[46] Cfr. L. LUPARIA, *La ratifica della Convenzione CyberCrime del Consiglio d'Europa*, cit., p. 720.

[47] Si può segnalare come talune *software house* manifestino talora un atteggiamento collaborativo con gli investigatori, rivelando al giudice richiedente i codici sorgente, a

Poiché la *beat stream image* è l'unica copia davvero identica all'originale, soltanto ad essa potrebbe essere riferita la denominazione di "copia clone" o di "copia forense" [48]. Dal canto suo, la legge n. 48 del 2008 non impiega tali locuzioni, optando per la più generica locuzione di "copia di dati" [49]. Si tratta di una scelta terminologica pragmatica, che sembra muovere dalla consapevolezza che se la copia forense è senz'altro la modalità duplicativa più garantistica dell'idoneità accertativa, non sempre è possibile ricorrere ad essa, in ragione dei tempi necessari per la sua realizzazione o a causa dei costi che la stessa comporta. In simili ipotesi si tratterà di capire se alle diverse copie realizzate corrisponda comunque una idoneità accertativa, verificando se i dati che inevitabilmente si sono alterati siano o meno rilevanti ai fini dell'accertamento del fatto.

b) Focalizzando l'attenzione sulla copia forense, occorre rilevare come la stessa rappresenti un'attività delicatissima. La giurisprudenza la qualifica come atto ripetibile [50]. In realtà, il quadro è assai articolato. Bisogna infatti distinguere tra dispositivi informatici spenti o accessi.

Nel primo caso la copia, se effettuata seguendo le *best practices*, si configura in effetti come un'attività ripetibile. Chiavi USB, schede di memoria *flash*, *hard disk* possono venire dunque copiati innumerevoli volte, senza rischi di alterazione dei dati.

condizione che venga mantenuto il segreto sugli stessi. Vi sono poi società che producono *tool open source*, di cui è quindi possibile conoscere anche i codici sorgente. Sul tema, cfr. F. CAJANI (a cura di), *Aspetti giuridici comuni delle indagini informatiche*, in S. ATERNO-F. CAJANI-G. COSTABILE-M. MATTIUCCI-G. MAZZARACO, *Computer forensics e indagini digitali, Manuale tecnico-giuridico e casi pratici*, vol. I, Experta, Forlì, 2011, p. 373 s.

[48] Nozione che corrisponde a quella di *digital evidence copy* rinvenibile nell'ISO 27037:2012, secondo la quale «*copy of the digital evidence that has been produced to maintain the reliability of the evidence by including both the digital evidence and verification means where the method of verifying it can be either embedded in or independent from the tools used in doing the verification*».

[49] In argomento, cfr. A.E. RICCI, Digital evidence *e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, p. 341.

[50] Per tutte, cfr. Cass., Sez. III, 8 luglio 2015, n. 29061, secondo la quale non integra un «accertamento tecnico irripetibile l'estrazione dei dati archiviati in un *computer*, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte».

Ben diversa, invece, l'ipotesi dei dispositivi accesi, rispetto ai quali la copia rappresenta di regola un atto irripetibile. Parimenti irripetibile appare pure l'attività di copia che, per essere effettuata, richieda l'accensione del dispositivo, come accade per gli *smartphone* [51]. Trattandosi di accertamenti tecnici irripetibili, si dovrebbe applicare la disciplina prevista dall'art. 360 c.p.p., la quale, come noto, implica che il pubblico ministero avvisi senza ritardo l'indagato, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo stabiliti per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici. A ciò si aggiunge la possibilità per la persona sottoposta alle indagini di formulare riserva di promuovere incidente probatorio. Si tratta di garanzie che in taluni casi potrebbero risultare inapplicabili a causa della necessità di effettuare nell'immediatezza la copia, pena la perdita di elementi di prova rilevanti a fini investigativi e magari idonei a dimostrare la non colpevolezza dell'indagato. Il legislatore ha poi previsto la possibilità di svolgere l'attività di copia anche ai sensi dell'art. 354 c.p.p., vale a dire come accertamento urgente [52]. In ogni caso, data l'irripetibilità dell'atto sarebbe quanto mai opportuno che l'inevitabile *deficit* di garanzie sia compensato dalla videoripresa dell'attività di copia svolta, al fine di consentire un contraddittorio almeno posticipato.

c) Poiché gli accertamenti tecnici possono accedere a mezzi tipici di ricerca della prova, si tratta di capire se anche la copia acceda a un istituto noto.

Generalmente, essa viene ritenuta una forma di sequestro. Orienterebbe in tal senso l'art. 254-*bis* c.p.p., che disciplina il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni, prevedendo che l'acquisizione dei medesimi possa anche avvenire «mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali». C'è però da chiedersi se una simile copia integri davvero una modalità di sequestro o non rappresenti piuttosto un autonomo atto investigativo di acquisizione dei dati.

[51] Al di là di tali distinzioni, occorre poi rilevare come l'irripetibilità dell'atto investigativo possa anche derivare dalle specificità del caso concreto.

[52] Sulle problematiche connesse alle attività informatiche urgenti, cfr. E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, cit., p. 135 ss.

Certo, la copia condivide con il sequestro la finalità di assicurare le cose che appaiono necessarie per l'accertamento del reato. Ma occorre ricordare che mentre il sequestro è un atto di coercizione reale che crea un vincolo di indisponibilità sulla *res* e ne determina lo spossessamento, la creazione della copia non determina invece simili conseguenze. Quest'ultima permette soltanto la duplicazione dei dati, mentre quelli originali restano nel possesso del soggetto. Infatti, a differenza del mondo fisico, dove la consegna di un oggetto implica necessariamente la privazione del suo possesso, nel mondo digitale la medesima azione può tradursi in una condivisione anziché in una privazione. A ciò si aggiunge che il sequestro è un atto di coercizione reale che incide sul diritto di proprietà e sulla libertà di iniziativa economica, mentre la copia clone non sembra comprimere simili diritti.

Esclusa la riconducibilità della copia alla disciplina del sequestro, ci si potrebbe chiedere se a tale atto investigativo risultino applicabili le norme in tema di ispezione o di perquisizione, sul presupposto che esse fanno espresso riferimento alle «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

In proposito occorrerebbe anzitutto rilevare che la copia non appare però un'attività ispettiva, trascendendo i limiti di un'attività descrittiva. Né sembrerebbe qualificabile in termine di rilievo o di operazione tecnica *ex* art. 244 comma 2 c.p.p., dato che il suo compimento si esplica in un'attività delicata, non meramente esecutiva, che richiede in capo all'investigatore capacità critica non elementare e specifiche competenze valutative.

In secondo luogo, la copia forense non sembrerebbe nemmeno ascrivibile alle perquisizioni, per il semplice motivo che essa è finalizzata alla duplicazione e non alla ricerca. Semmai, essa rappresenta spesso un'attività prodromica alla perquisizione, rispetto alla quale resta però chiaramente distinta.

Ciò premesso, se è vero che per istituto giuridico si può intendere un *quid* unitario, alla luce del quale le norme «assumono valore e significato, in quanto create, non come un'artificiosa congerie di particolari, ma in funzione della natura e degli scopi»[53] dell'attività investigativa, la copia forense sembra a tutti gli effetti integrare un nuovo istituto giuridico, contraddistinguendosi per autonoma funzione rispetto alle altre tipologie di indagine e per un'autonoma struttura. Una simile ragione induce perciò ad auspicare un intervento legislativo volto a disciplinare in maniera autonoma la copia forense.

[53] Così A. TRABUCCHI (a cura di), *Istituzioni di diritto civile*, quarantesima seconda edizione, Cedam, Padova, 2005, p. 11.

d) Si può infine riporre l'attenzione su una particolare prassi. Non di rado un dispositivo informatico viene sequestrato per procedere poi a copia del suo contenuto. A quel punto, il dispositivo informatico viene restituito, mentre si trattiene la copia. Correttamente le Sezioni Unite hanno escluso che quest'ultima sia riconducibile alla disciplina dettata dall'art. 258 c.p.p. in ordine alle copie dei documenti sequestrati[54], sul presupposto che un dispositivo informatico non sembra certo equiparabile ad un documento.

A fronte della restituzione del dispositivo e del trattenimento della copia previamente estratta si pone però il problema di comprendere se permanga o meno l'interesse ad impugnare e se sia possibile esperire il riesame per la restituzione della copia. Dissequestro e restituzione sono infatti due atti profondamenti diversi[55]. Sul piano dell'interesse ad impugnare, non v'è dubbio che esso sussista, almeno come interesse a riottenere la disponibilità esclusiva del «patrimonio informativo» contenuto nella copia clone[56]. Una lettura convenzionalmente conforme[57] dei rimedi esperibili sembrerebbe, poi, portare ad estendere l'applicabilità della disciplina del riesame anche alla copia[58]. Dal canto suo, la

[54] Cfr. Cass., Sez. Un., 20 luglio 2017, n. 40963.

[55] In questo senso, cfr. Cass., Sez. Un., 24 aprile 2008, n. 18253.

[56] Tale interesse è stato riconosciuto anche da Cass., Sez. Un., 20 luglio 2017, n. 40963. In argomento, cfr., S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, cit., p. 478, nonché P. RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico*, in *Cass. pen.*, 2018, p. 131 ss.

[57] Cfr. Corte eur., 7 giugno 2007, *Smirnov* c. *Russia*; Id., 22 maggio 2008, *Ilya Stefanov* c. *Bulgaria*; Id., Grande Camera, 14 settembre 2010, *Sanoma Uitgevers, B.V.* c. *Paesi Bassi*; Id., 19 giugno 2014, *Draghici* c. *Portogallo*; Id. 19 gennaio 2016, *Gulcu* c. *Turchia*; Id., 2 aprile 2015, *Vinci Construction, GTM Génie Civil, Services* c. Francia.

[58] Invero, l'«interpretazione conforme, ponendosi come snodo cruciale nella complessa interazione tra diritto europeo e ordinamenti statuali, si presenta come uno strumento al contempo prezioso e delicato. Prezioso perché, sollecitando i giudici

Corte di Giustizia ha però rimarcato il divieto di interpretazioni *contra legem* giustificate sull'interpretazione convenzionalmente conforme, dato che quest'ultima «deve restare appunto uno strumento ermeneutico che si "mantiene" e che opera pur sempre nell'ambito della "legge"»[59].

Proprio quest'ultimo profilo sembra rappresentare il fattore dirimente in materia. Estendere il riesame anche alla restituzione della copia clone si "mantiene" davvero all'interno della norma che prevede il riesame o ne fuoriesce? Non vi è forse nel nostro ordinamento un principio di tassatività delle impugnazioni, che impedisce estensioni analogiche?

A rigore, il percorso argomentativo sembrerebbe dover essere il seguente. Considerato il principio di tassatività delle impugnazioni non appare legittimo un riesame finalizzato a consentire la restituzione della copia clone. Né sarebbe possibile un'interpretazione convenzionalmente conforme in quanto *contra legem* perché idonea a vulnerare il principio di tassatività. A meno di ignorare l'esistenza del divieto di interpretazione *contra legem*, a volte rinnegato dalla stessa Corte di Giustizia che ne afferma l'esistenza, come è avvenuto nel noto caso Pupino[60].

Volendo tenere però fermo tale principio, ne deriva un assetto assai censurabile, sia per le frizioni con l'art. 3 Cost. sul piano della disparità di trattamento rispetto alla disciplina del sequestro; sia in rapporto alla Convenzione europea dei diritti dell'uomo, almeno per i profili di tensione che si determinano in ordine all'equità processuale ai sensi dell'art. 6 Cedu, senza contare che, a seconda delle specifiche situazioni, potrebbero venire in rilievo anche referenti convenzionali diversi come l'art. 8 Cedu. Di qui la necessità di un intervento legislativo atto a pre-

nazionali a rileggere le norme interne alla luce delle indicazioni e degli obiettivi europei, potrà favorire lo sviluppo in senso comunitariamente (e convenzionalmente) orientato dei processi penali nazionali (...). Ma l'interpretazione conforme è pure uno strumento molto delicato, perché è suscettibile di mettere anche in forte tensione "legalità interna" e "legalità europea"». Così, R.E. KOSTORIS, *Il sistema dell'Unione*, in ID. (a cura di), *Manuale di procedura penale europea*, III ed., Giuffrè, Milano, 2017, p. 43.

[59] In questi termini R.E. KOSTORIS, *ult. cit.*, p. 45.

[60] Corte giust., 16 giugno 2005, C-105/03, Pupino.

vedere espressamente la possibilità di esperire il riesame per la finalità di restituzione della copia[61].

8. *Profili peculiari in tema di richiesta di consegna ed esame presso banche di dati informatici.*

Nell'ambito dei mezzi di ricerca della prova, l'art. 248 c.p.p. disciplina al comma 1 la richiesta di consegna di una cosa determinata[62], mentre prevede al comma 2 l'esame presso banche di atti, documenti e corrispondenza, nonché di dati, informazioni e programmi informatici.

La richiesta di consegna può essere rivolta dall'autorità giudiziaria quando si ricerchi una cosa determinata. Se la cosa viene presentata, l'autorità può non procedere a perquisizione o effettuarla ugualmente, qualora risulti utile alla completezza delle indagini. Il vaglio tra l'una o l'altra possibilità avviene sulla base di una scelta discrezionale[63] da parte dell'autorità giudiziaria o dell'ufficiale di polizia giudiziaria delegato al compimento dell'atto[64]. «Valido, comunque, il rilievo che la perquisizione, proprio perché incide su sfere costituzionalmente garantite, dovrebbe essere eseguita solo se gli altri strumenti previsti dal legislatore per ottenere il medesimo risultato finale si siano in concreto rivelati infruttuosi»[65].

Poiché la legge n. 48 del 2008 ha previsto espressamente la possibilità di esaminare presso le banche anche «dati, informazioni e programmi

[61] Anche in considerazione del fatto che qualora si effettui la copia dei dati di un terzo, quest'ultimo, non rivestendo alcun ruolo nel procedimento penale, non potrebbe in alcun modo far valere i suoi diritti.

[62] Rileva come tale previsione si caratterizzi per il «vuoto» del suo contenuto e sia indicativa di una prosa «a maglie larghe», dato che riporta delle mere scelte operative, F. CORDERO, *Procedura penale*, cit., p. 834.

[63] Pone in luce come sarebbe invece opportuno che tale opzione fosse obbligatoria, G. BELLANTONI, *Sequestro probatorio e processo penale*, La Tribuna, Piacenza, 2005, p. 48.

[64] Per tutti, cfr. M. BARGIS, voce *Perquisizione*, cit., p. 492.

[65] In questi termini, M. BARGIS, voce *Perquisizione*, cit., 1995, p. 492.

informatici» (art. 248 comma 2 c.p.p.), ma non ha fatto alcun riferimento alla richiesta di consegna dei dati informatici, sorge il dubbio se sia possibile rivolgere quest'ultima richiesta. Per impostare una risposta al problema, occorre ricordare che la richiesta di consegna può essere effettuata, come si è detto, quando per mezzo della perquisizione si ricerchi «una cosa determinata». Tutto dipende, quindi, dalla latitudine che si intende attribuire a tale ultima nozione.

In proposito, si può ricordare come nell'ambito del codice penale si tenda ad accogliere una nozione restrittiva. In tale prospettiva si è, ad esempio, escluso che dati, informazioni e programmi informatici possano essere ricondotti nella nozione di «cosa» rilevante ai fini del danneggiamento *ex* art. 635 c.p.p.[66], tanto che il legislatore ha dettato un'apposita e distinta disciplina riguardante il danneggiamento di dati e programmi informatici, ai sensi dell'art. 635-*bis* c.p. Sulla stessa linea si è posta poi la disciplina dell'art. 392 c.p. in tema di esercizio arbitrario delle proprie ragioni con violenza sulle cose.

L'approccio del legislatore in materia processuale penale sembra però caratterizzarsi per una minore restrittività. Lo si è visto in tema di sequestro, nel cui contesto pare senz'altro possibile ricondurre al concetto di «cosa» anche dati, informazioni e programmi. Analogamente, in tema di perizia, è ormai pacifico che tale mezzo di prova possa essere disposto anche in riferimento a dati informatici[67]. A differenza del diritto penale sostanziale, quindi, nel diritto processuale penale sembra essere ormai accolta una nozione ampia di «cosa», che è senz'altro idonea a ricomprendere anche i dati informatici. Opzione interpretativa che pare dunque riferibile anche alla richiesta di consegna, dove i problemi si incentrano semmai sulla necessità che dalla consegna non derivi una alterazione dei dati stessi.

Al riguardo, occorre rilevare che la consegna dei dati digitali può es-

[66] Cfr. C. PECORELLA, *Diritto penale dell'informatica. Ristampa con aggiornamento*, Cedam, Padova, 2006, p. 204, secondo la quale prima dell'introduzione dell'art. 635-*bis* c.p. solo alcuni dati e programmi informatici, «– e comunque a prezzo di discutibili acrobazie interpretative – potevano (...) ricondursi alla fattispecie tradizionale».

[67] Si pensi, ad esempio, ad una perizia che abbia ad oggetto fotografie digitali inserite in *social network*. Potendo essere qualificate in termini di «cose», tali fotografie potrebbero poi essere oggetto di esame da parte dei consulenti tecnici nominati dopo l'esaurimento delle operazioni peritali che siano al riguardo autorizzati dal giudice.

sere effettuata in due modi: mediante consegna del dispositivo o del supporto in cui sono contenuti i dati o mediante copia dei dati. In quest'ultimo caso, solo una copia effettuata seguendo determinate procedure rappresenterà un secondo originale e sarà, quindi, idonea a garantire l'integrale genuinità dei dati consegnati. Peraltro, poiché il soggetto che effettua la consegna, almeno di regola, non è in grado di fare una simile copia, si tratterà di capire di volta in volta se la metodologia seguita possa inficiare gli elementi di prova che sono rilevanti ai fini dell'indagine nel caso di specie. Da questo punto di vista, infatti, anche se la copia non rappresentasse un secondo originale, ma i dati alterati fossero irrilevanti per il procedimento penale, essa potrebbe rappresentare comunque una modalità valida di consegna, rispetto alla quale andrebbe però sempre preferita, laddove possibile ed adeguata alla situazione, la *beat stream image*, vale a dire la copia in grado di garantire l'identità all'originale.

Infine, ci si può chiedere se i provvedimenti con i quali si richieda la consegna di dati, informazioni e programmi di una cosa determinata ai sensi dell'art. 248 c.p.p. siano soggetti a riesame. Nel caso di consegna di un intero dispositivo o del supporto informatico si determinerebbe un effetto ablativo della *res*, dato che la richiesta di consegna sembra caratterizzarsi per la sua assimilabilità sostanziale ad un provvedimento di sequestro a causa dell'analogo effetto pratico rappresentato dalla sottrazione della libera disponibilità del bene al destinatario dell'atto. Anche nel caso di consegna di copia di dati, poi, potrebbe sussistere un interesse alla restituzione al fine di ottenere la non conoscibilità dei dati contenuti nella copia.

La giurisprudenza esclude la possibilità di riesame[68], sottolineando che quest'ultimo è ammesso soltanto in ordine a provvedimenti che presentino sia i requisiti sostanziali che formali del sequestro[69]. Secondo la giurisprudenza, sequestro e richiesta di consegna non potrebbero infatti in alcun modo essere omologati a causa della natura autoritativa del primo, che si contrapporrebbe alla spontaneità della seconda.

In realtà, la preclusione al riesame del provvedimento di richiesta di

[68] Cfr. Cass., Sez. III, 11 aprile 2017, n. 37135.

[69] Cfr. Cass., Sez. V, 20 giugno 1995, n. 1834.

consegna sembra derivare dal principio di tassatività dei mezzi di impugnazione. A meno di non ritenere la richiesta di consegna un atto complesso, che assomma in sé anche il sequestro, avverso il provvedimento di richiesta di consegna non sembra quindi esperibile il riesame per il semplice motivo che nessuna norma lo prevede e, in materia, risulta vietata ogni forma di analogia. Sul piano dei gravami sembra però delinearsi una irragionevole disparità, censurabile *ex* art. 3 Cost., tra la disciplina del sequestro e quella della richiesta di consegna, dato che a parità di effetto ablativo della *res* dovrebbe corrispondere analoga possibilità di riesame.

Passando ad esaminare la disciplina dell'esame presso banche[70] occorre ricordare come, a seguito della legge n. 48 del 2008, sia stato previsto che tale esame possa riguardare anche dati, informazioni e programmi informatici.

C'è chi ha posto in luce che una simile eventualità doveva ritenersi consentita già nel previgente assetto normativo. Ad ogni modo, per fugare ogni dubbio, il legislatore ha comunque ritenuto opportuno prevederla espressamente. Al fine di rintracciare le cose da sequestrare o per accertare circostanze utili per le indagini l'art. 248 comma 2 c.p.p. prevede, poi, la possibilità di procedere a perquisizione soltanto nel caso di rifiuto di consentire l'esame presso la banca. Diversamente da quanto previsto per la richiesta di consegna, non è rimessa all'autorità giudiziaria o agli ufficiali di polizia giudiziaria da questa delegati alcuna scelta discrezionale tra l'esame e la perquisizione, dato che quest'ultima è subordinata al rifiuto dell'esame.

9. *Le intercettazioni telematiche: le ragioni della disciplina ed il suo nucleo oggettivo.*

Nell'originaria disciplina codicistica non figurava alcuna norma specificamente dedicata alle intercettazioni telematiche. Compariva,

---

[70] Occorre rilevare come il termine «banche» vada inteso in senso restrittivo, riferendolo ai soli istituti di credito e non certo anche alle «banche dati». Al riguardo, cfr. Cass., Sez. IV, 17 aprile 2012, n. 19618.