Capitolo 16
LA PROVA DIGITALE

di Luigi Cuomo

I sistemi informatici e telematici costituiscono gli strumenti mediante i quali vengono svolte le principali attività lavorative, sociali e personali degli utenti, ma anche i mezzi con cui vengono stipulati contratti, modificate sfere giuridiche e compiuti atti illeciti, per cui l'ambito della prova scientifica è stato esteso alla prova digitale, che riguarda l'acquisizione dei dati, la conservazione delle informazioni e la documentazione dei contenuti multimediali archiviati all'interno dei dispositivi elettronici, che, in maniera sempre più ampia, interessano a fini di indagine la polizia giudiziaria, gli operatori del diritto e l'autorità giudiziaria

Sezione I
La prova digitale

1. La prova digitale e l'ambiente informatico

Le sfide che la modernità pone all'operatore del diritto derivano dalla diffusione esponenziale degli strumenti tecnologici e dalla loro capacità di influenzare la vita delle persone.

Le attività, le conoscenze e le decisioni dell'individuo dipendono sempre più dalla tecnologia informatica e dai processi di trattamento automatizzato delle informazioni.

La nascita delle investigazioni digitali è strettamente dipendente dalla diffusione del crimine informatico e dalla codificazione di nuove fattispe-

cie di reato, fino al punto di considerare l'elaboratore elettronico come un contenitore di informazioni o una vera e propria fonte di prova.

L'utilizzo sempre più esteso del computer ha fatto diffondere una serie di condotte antigiuridiche, convenzionalmente fatte ricadere sotto la dizione di crimini informatici (*computer's crimes*), in cui vengono ricompresi sia i fatti illeciti nei quali l'elaboratore riveste il ruolo di strumento attivo, inteso come mezzo per la commissione di reati, che di oggetto diretto di tutela, in cui il sistema elettronico risulta l'obiettivo dell'altrui condotta illecita[1].

L'ingresso dell'informatica nell'ambito della vita commerciale e di relazione ha dato luogo a situazioni nelle quali atti e negozi giuridici sono direttamente regolati e conclusi attraverso ordini impartiti ad elaboratori elettronici, che provvedono a modificare sfere giuridiche e ad eseguire trasferimenti di capitali in forma immateriale[2].

La tecnologia non è più solo uno strumento a disposizione dell'uomo, ma è diventata l'ambiente che lo circonda in una dimensione nella quale le esigenze dell'utente appaiono subordinate alle regole di funzionamento degli strumenti di comunicazione.

Gli apparecchi elettronici costituiscono strumenti di percezione e, al tempo stesso, di creazione dello spazio virtuale generato dalle interazioni che vengono a stabilirsi tra le macchine e gli utenti: l'informatica, unitamente alla telefonia, è diventata la piattaforma in cui viene svolta la maggior parte delle attività lavorative, sociali e personali[3].

---

[1] Nella storia dell'informazione umana, l'organizzazione e la trasmissione dell'esperienza è avvenuta attraverso la vista (la dimostrazione gestuale, la segnalazione ottica a distanza, la scrittura) e l'udito (il linguaggio parlato, la segnalazione sonora a distanza, la registrazione fonica). Nella società industriale, con la scoperta dell'elettricità si è fatto ricorso a strumentazioni tecniche che hanno consentito nuove forme di trasporto del messaggio visivo o auditivo con l'uso del telegrafo e del telefono, i quali rappresentarono i precedenti sistemi di codificazione dell'informazione con impulsi elettromagnetici, seguiti dalle invenzioni della radio e della televisione, con le quali si verificò una modificazione dell'informazione; giacché essa divenne da biunivoca (da punto a punto fra emittente e ricevente) una comunicazione onnicentrica, cioè diffusa e ricevibile da ogni punto» (V. Frosini, voce *Telematica e Informatica Giuridica*, in *Enc. dir.*, vol. XLIV, Milano, 1992, p. 60).

[2] M. M. Alma - C. Perroni, *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. pen. e proc.*, 1997, p. 504; E. Giannantonio, *L'oggetto giuridico dei reati informatici*, in *Cass. pen.*, 2001, p. 2029; G. Paterna, «New economy» *e* «cybercrimine», in *Criminologia psicopat. forense*, 2000, 16, p. 50; G. Di Giandomenico - L. Cuomo (a cura di), *Profili giuridici dell'informatica*, Edizioni Scientifiche Italiane, Napoli, 2000, p. 153.

[3] In tema v. A. Valastro, *La tutela penale delle comunicazioni intersoggettive, fra evoluzione tecnologica e nuovi modelli di responsabilità*, in *Riv. it. dir. proc. pen.*, 1999, p. 989; R. Frank, *Tutela della riservatezza e sviluppo tecnologico*, in *Giust. civ.*, 1987, p. 26.; R. Galli, *Alcune note sulla* «privacy» *(legge n. 675 del 1996)*, in *Foro pad.*, 1998, p. 121; V. Grippo, *Analisi dei dati personali presenti su Internet. La legge n. 675/96 e le reti telematiche*, in *Riv. critica dir. priv.*, 1997, p. 639; V. Librando, *La tutela della riservatezza nello sviluppo tecnologico*, in *Dir. inf.*, 1987, p. 487; L. Cuomo - B. Izzi, *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, in *Cass.*

I sistemi sono costituiti da elaboratori elettronici che rispondono ai comandi impartiti da soggetti in possesso di una preparazione tecnica adeguata al trattamento delle informazioni e all'impiego delle risorse informatiche[4]. Il comando (*input*) rivolto al computer corrisponde a un atto umano consapevole e volontario, che si traduce in un messaggio diretto a trasferire la volontà dall'utente all'elaboratore elettronico, il quale, a sua volta, procede automaticamente alle operazioni di codificazione, decodificazione, trattamento, trasmissione o memorizzazione di dati.

Sotto il profilo ontologico, il comando rappresenta uno degli elementi costitutivi dei reati informatici, che si connota per l'estrinsecazione di un atto di volontà dell'operatore attraverso un impulso elettronico diretto al computer.

Tutte le azioni che avvengono in rete assumono l'aspetto di comportamenti comunicativi, che consistono nella trasmissione o nel trasferimento di dati elettronici, come le istruzioni che vengono scambiate tra i sistemi informatici per coordinarne il reciproco funzionamento o i contenuti multimediali che sono trasmessi tra gli utenti che utilizzano la medesima tecnologia.

---

pen., 2002, p. 1018. Nel corso degli anni si è modificato il rapporto "uomo-computer", considerato che, se in origine era effettivamente un mezzo per svolgere una attività professionale, attualmente è un vero e proprio ambito spaziale all'interno del quale l'individuo proietta tutta la sua personalità. È allora facile immaginare che a breve non avrà più senso distinguere tra domicilio comune e domicilio informatico, nel senso che quest'ultimo si avvicinerà come contenuti sempre più al primo, con la conseguenza che i criteri da seguire per apprestare adeguata protezione saranno meno incerti rispetto a quanto accade oggi» (P. Galdieri, *Il domicilio informatico: l'interpretazione dell'art. 615-ter cod. pen. tra ragioni di carattere sistematico e forzature*, in *Dir. inf.*, 2013, p. 88 ss.).

[4] L'espressione «sistema informatico», esprime «il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche» (Cass. pen., Sez. VI, 4 ottobre 1999, n. 3065, in *Cass. pen.*, 2001, p. 481). La definizione offerta dalla giurisprudenza è fondata sul passaggio dal «dato» all'«informazione», nel senso che alla funzione di registrazione e di memorizzazione elettronica dei dati come rappresentazione elementare di un fatto, si affianca l'attività complementare di elaborazione e di organizzazione logica, con formazione di un insieme coordinato di informazioni (R. Borruso - G. Buonomo - G. Corasaniti - G. D'Aietti, *Profili Penali dell'informatica*, Giuffrè, Milano, 1994, p. 4). Le Sezioni Unite hanno precisato che "un sistema informatico è costituito dalle componenti *hardware* e *software*, le prime rappresentate, secondo la comune definizione, dal complesso di elementi fisici non modificabili (quali circuiti, unità di memoria, parti meccaniche etc.), cui si aggiungono periferiche di ingresso (ad. es. tastiera, *scanner* etc.) e di uscita (es. *monitor*, stampante) ed altri componenti comuni (*modem*, masterizzatore, cavi) e le seconde costituite, sempre secondo la comune accezione, dall'insieme di istruzioni e procedure necessarie per il funzionamento stesso della macchina (*software* di base) o per farle eseguire determinate attività (*software* applicativo) e costituiti da programmi o dati memorizzati su specifici supporti (Cass., Sez. un., 20 luglio 2017, n. 40963; in senso analogo, Cass., Sez. V, 8 gennaio 2020, n. 4470).

Il soggetto attivo è in grado di agire contemporaneamente sia sul computer di partenza, che sulla postazione remota del soggetto destinatario dei dati: in tal modo l'azione si moltiplica nello spazio e produce simultaneamente le conseguenze volute dall'operatore in entrambi i luoghi dove si trovano i sistemi di elaborazione.

Un sistema informatico, un computer portatile e uno smartphone conservano nella memoria interna una ingente massa di dati relativi al loro utilizzo, che consentono di risalire ad ogni attività che è stata espletata con il dispositivo[5]. Per questo motivo, i computer possono essere gli strumenti necessari per la commissione di reati (soggetto attivo di delitti), possono contenere la prova della consumazione di crimini di tipo tradizionale (testimoni di delitti), oppure possono essere l'obiettivo di atti illeciti (soggetto passivo di delitti).

Le prove che i sistemi informatici contengono al loro interno non sono altro che cariche elettromagnetiche, perché le informazioni come una immagine, un suono, una sequenza video, un testo o un'altra rappresentazione del pensiero umano subiscono un processo di conversione in una sequenza di *bit*, risultanti dalla magnetizzazione o smagnetizzazione della superficie di un supporto o dalla variazione dello stato fisico della materia.

I *bit* qualora rappresentino atti, fatti o dati giuridicamente rilevanti, costituiscono un documento elettronico ai sensi dell'art. 1, lett. *p*), D.Lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale)[6].

La prova elettronica[7], ai fini della sua conoscibilità esterna e dell'equivalenza al documento informatico, è la rappresentazione di un fatto (art. 234 c.p.p.), ovvero tutto ciò che può essere oggetto di prova *ex* art. 192 c.p.p. incorporata in una base materiale con metodo digitale.

La caratteristica fondamentale di un'informazione digitalizzata risiede nella possibilità di scorporarne il contenuto rappresentativo dal supporto su cui è stata originariamente memorizzata e, quindi, l'esistenza dell'una prescinde dalla rilevanza dell'altro.

---

[5] Alla sempre più avvertita percezione sociale della gravità della fenomenologia criminosa che si manifesta nel «*ciberspazio*» si contrappone la problematicità di "isolare" il soggetto attivo del reato, ovvero l'autore materiale dei contenuti illeciti circolanti in rete: è sufficiente ricordare la possibilità per l'utente di fornire – al momento della registrazione – falsi estremi di identità, di sottrarre il proprio nome di accesso o la «*password*», oppure di alterare fraudolentemente il rispettivo indirizzo elettronico (F. Ruggiero, *Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'*internet provider, in *Giur. mer.*, 2001, p. 586).

[6] Sul concetto di documento v. P. Guidi, *Teoria giuridica del documento*, Milano, p. 36; F. Carnelutti, *La prova civile. Parte generale. Il concetto giuridico della prova*, Giuffrè, Milano, p. 138; S. Campanella, *Profili problematici in tema di documenti dichiarativi*, in *Ind. pen.*, 2008, p. 118.

[7] Ben può essere utilizzata la formula *digital evidence* o prova digitale, quale recipiente ove includere ogni forma di utilizzo a fini procedimentali, in senso lato, di dati originariamente contenuti in supporti informatici o telematici.

Si può considerare prova digitale ogni informazione probatoria la cui rilevanza processuale dipende dal contenuto del dato o dalla particolare allocazione su una determinata periferica, ovvero dalla trasmissione secondo modalità informatiche o telematiche (come *sms*, messaggi scambiati tramite piattaforme digitali, *chat*, pagine *internet*, *social network*)[8].

Le prove digitali, costituite da *record*, *file*, codici sorgente, tracce digitali, programmi informatici e flussi di *bit*, per la loro natura immateriale variamente rappresentabile, sono raccolte in un luogo virtuale dove perde consistenza la naturale propensione dell'uomo a rapportarsi con il mondo circostante con l'uso dei sensi e, in particolare, con il tatto.

Il *file*, pur non potendo essere materialmente percepito dal punto di vista sensoriale, possiede una dimensione fisica costituita dalla grandezza dei dati che lo compongono, come dimostrano l'esistenza di unità di misurazione della capacità di un *file* di contenere dati e la differente grandezza dei supporti fisici in cui i *files* possono essere conservati ed elaborati.

A conclusione di un articolato percorso ermeneutico, in giurisprudenza è stato recentemente affermato che, se anche difetta il requisito dell'apprensione materialmente percepibile di un *file* in sé considerato (se non quando esso sia fissato su un supporto digitale che lo contenga), il flusso dei dati (al pari degli altri beni e dell'energia) rappresenta una cosa mobile, definibile quanto alla sua struttura, alla possibilità di misurarne l'estensione e la capacità di contenere informazioni, suscettibile di essere trasferito da un luogo ad un altro, anche senza l'intervento di strutture fisiche direttamente apprensibili dall'uomo[9]. L'elemento digitale è comunque un'entità fisica, la quale può possedere i requisiti della mobilità, identificabile nell'autonoma esistenza e nella delimitazione spaziale.

Come la cosa mobile, il dato espresso da una cifra binaria è un'entità spazialmente definita: esso è delimitato fisicamente all'interno del computer, ove assume una forma significativa fra quelle descritte ed occupa una porzione quantitativa di memoria.

Il dato informatico mantiene tale delimitazione anche quando è trasmesso da un computer all'altro: in tal caso esso perde la consistenza significativa che possedeva all'interno di una determinata area di memoria e si scompone in singoli pacchetti, costituenti parimenti entità fisicamente delimitate, che si indirizzano nei confronti di un sistema operativo (ad esempio un *server*) capace di ricomporli nella forma originaria.

---

[8] A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, 2023, Torino

[9] Integra il delitto di appropriazione indebita la sottrazione definitiva di "dati informatici" o "*file*" mediante copiatura da un "*personal computer*" aziendale, affidato all'agente per motivi di lavoro e restituito con "*hard-disk*" formattato, in quanto i "dati informatici", per fisicità strutturale, possibilità di misurarne le dimensioni e trasferibilità da un luogo all'altro, sono qualificabili come cose mobili ai sensi della legge penale (Cass., Sez. II, 7 novembre 2019, n. 11959).

Come la cosa mobile, inoltre, il dato è una entità autonoma e ciò è dimostrato dal fatto che le informazioni possono essere in sé trasferite da un luogo all'altro del *computer* oppure spedite essendo simile, sotto il profilo della materialità – fisicità – corporalità, a qualunque altro bene immateriale. Ai fini della tutela penalistica e, in particolare, dei reati contro il patrimonio, l'ampliamento della gamma delle attività che l'uomo è in grado di svolgere mediante le apparecchiature informatiche, determina la necessità di considerare in modo più appropriato i criteri classificatori utilizzati per la definizione di nozioni che non possono rimanere immutabili nel tempo, essendo evidente che il dato informatico possiede tutti i requisiti della mobilità della cosa[10].

La registrazione di dati nelle memorie di un *computer* è un modo di scrivere rivoluzionario: con un nuovo alfabeto (quello dei *bit*), con un inchiostro alternativo (il flusso degli elettroni) e su supporti diversi (memorie elettroniche, magnetiche o ottiche).

Le informazioni digitalizzate presentano le caratteristiche della fulmineità della riproduzione da una memoria all'altra, della conversione in dati intellegibili all'uomo, della mobilità dei caratteri e della miniaturizzazione dei supporti.

Il documento informatico è dematerializzato ed è facilmente modificabile o alterabile, perché esiste a prescindere dal supporto e dalla base materiale che eventualmente lo incorpora (*hard disk*, *pen drive*, *cd*, *dvd*) e, a differenza del documento analogico, contiene molti più dati (orario e data di formazione o autore) che devono essere preservati ai fini dell'attendibilità del risultato probatorio.

In questo contesto la polizia giudiziaria ha l'esigenza di valutare il ruolo e la natura delle "impronte elettroniche", di individuare quali supporti informatici possono contenere potenziali tracce del reato, di acquisire e preservare le fonti di prova fino alla loro successiva analisi laddove non fosse possibile espletare i dovuti accertamenti direttamente sul posto.

La pseudo-immaterialità del processo di formazione della prova rende necessaria una nuova regolamentazione della materia o l'aggiornamento delle norme preesistenti[11].

---

[10] L'uomo ha imparato a materializzare le entità astratte, per rendere possibile la loro manifestazione in modo più efficace e duraturo dell'espressione orale, per conservare la prova del loro contenuto, o per dare al soggetto un simbolo concreto rappresentativo del suo diritto. In dottrina, v. N. Pisani, *La nozione di "cosa mobile" agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica*, in *Dir. pen. e proc.*, 2020, p. 651; M. Carani, *L'appropriazione indebita dei dati informatici: perché i files si possono considerare cose mobili*, in *Cass. pen.*, 2020, p. 4152; R. Cappitelli, *I confini della nozione di bene mobile nei delitti contro il patrimonio*, in *Cass. pen.*, 2021, p. 924; A. Scarcella, *Dato informatico, nozione penale di cosa mobile ed appropriazione indebita*, in *Cass. pen.*, 2021, p. 556.

[11] F. Berghella - R. Blaiotta, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, p. 2329; F. Bravo, *Crimini informatici e utilizzo dei mezzi di ricerca della prova nella condu-*

L'attendibilità del contributo probatorio, non umano ma tecnologico, dipende essenzialmente dalla capacità tecnica degli organi inquirenti, che devono essere in grado di interrogare il *computer*, al fine di identificare e preservare al suo interno gli elementi utili alla ricostruzione del fatto.

Ogni sistema informatico è dotato di una ampia memoria, che non solo archivia i dati utilizzati in modo ricorrente, ma registra anche una molteplicità di informazioni relative a tutte le operazioni che l'utente ha svolto nel corso del suo utilizzo.

Anche se viene compiuta una operazione di cancellazione, i dati non sono definitivamente eliminati dall'elaboratore elettronico ma, a determinate condizioni, possono essere riportati alla luce e utilizzati a fini di indagine.

Lo studio di questo settore è affidato alla *computer-forensics*, che si occupa della preservazione, dell'identificazione, dell'acquisizione, della conservazione e della documentazione dei contenuti degli elaboratori elettronici o dei sistemi informativi in generale, allo scopo di evidenziare prove a fini di indagine.

La peculiarità delle indagini nel settore dei reati informatici ha indotto gli operatori a coniare i termini di "informatica forense" (*digital forensics* o *computer forensics*) e di prova digitale (*digital evidence*), che indicano determinate fasi in cui si articola un'indagine informatica.

Non esiste una metodologia condivisa per il trattamento delle prove digitali, ma vengono utilizzati un insieme di strumenti e talune procedure consolidatesi nella prassi con la sperimentazione.

In un'indagine informatica, per le cognizioni tecniche implicate, è necessariamente coinvolta una molteplicità di figure professionali (ufficiali e agenti di polizia giudiziaria; ausiliari di polizia giudiziaria; consulenti tecnici, periti, esperti informatici).

L'obiettivo principale di un'indagine in ambito digitale è la preservazione, l'identificazione e la documentazione delle attività che sono state compiute con un sistema informatico o telematico al fine di acquisire la prova della colpevolezza o dell'innocenza dell'indagato.

La prova digitale, per l'elevato grado di tecnicismo richiesto per trasformare le informazioni originariamente contenute nei sistemi informatici in informazioni e dati comprensibili dal giudice, rientra nella categoria della prova scientifica[12].

---

zione delle indagini, in *Riv. giur. polizia*, 1998, p. 711; F. Buffa, *Internet e criminalità*, Milano, 2001; C. Serra - M. Strano, *Nuove frontiere della criminalità*, Milano, 1997. M. Luberto - G. Zanetti, *Il diritto penale nell'era digitale. Caratteri, concetti e metafore*, in *Indice pen.*, 2008, p. 497; O. Dominioni, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, Milano, 2005, p. 117.

[12] F. Casasole, *Le indagini tecnico-scientifiche: un connubio tra scienza e diritto in perdurante attesa di disciplina*, in *Dir. pen. proc.*, 2008, 11, p. 1443. F. Auletta, *La prova scientifica: diritto,*

Tuttavia, il baricentro di un processo fondato sulla prova scientifica si colloca sempre più nelle indagini preliminari, in cui il dato digitale viene di regola acquisito dalla polizia giudiziaria e successivamente analizzato da personale tecnico.

Il dato digitale presenta i caratteri della immaterialità e della fragilità, per cui può essere facilmente modificato o cancellato da personale non in possesso di conoscenze tecniche adeguate[13].

Per tali ragioni, l'acquisizione e la conservazione della prova informatica deve avvenire attraverso un processo volto alla manipolazione controllata dei dati, che sia in grado di fornire adeguate garanzie di integrità, autenticità e disponibilità delle informazioni[14].

La volatilità del dato digitale e la sua modificabilità nel tempo, in caso di reperto informatico erroneamente acquisito, conservato o analizzato con metodologie inappropriate, potrebbe determinare una inattendibilità delle informazioni poste a disposizione del giudice[15].

Un corretto procedimento di analisi forense dei dati elettronici prevede l'esecuzione delle seguenti attività: 1) riconoscimento e identificazione della fonte di prova; 2) acquisizione del dato o del sistema; 3) conservazione e protezione delle informazioni; 4) valutazione dei risultati sotto il profilo tecnico, giuridico e investigativo; 5) presentazione dei risultati al pubblico ministero, al giudice o al committente in caso di attività stragiudiziale.

In considerazione della fragilità dei dati, sono molteplici le garanzie previste dal sistema processuale:

– il dovere di conservare inalterato il dato informatico originale nella sua genuinità (garanzia prevista per le ispezioni e perquisizioni, anche della polizia giudiziaria, dagli artt. 244, comma 2, 247, comma

---

epistemologia, strumenti d'acquisizione, in *Riv. trim. dir. proc. civ.*, 2016, p. 461; G. Ubertis, *Prova scientifica e giustizia penale*, in *Riv. it. dir. proc. pen.*, 2016, p. 1192; A. Scaglione, *Profili problematici della prova scientifica nel processo penale*, in *Giust. pen.*, 2016, p. 571; P. Moscarini, *Lo statuto della "prova scientifica" nel processo penale*, in *Dir. pen. proc.*, 2015, p. 649.

[13] Le difficoltà operative sono legate alla natura stessa della scena del crimine digitale, localizzata tra i polpastrelli dell'autore e la tastiera, tra i suoi occhi e le emissioni elettromagnetiche del «*monitor*». Senza contare, poi, le innumerevoli possibilità di anonimizzazione e di sostituzione dell'identità altrui offerte dall'ambiente digitale (L. Marafioti, *Digital evidence e processo penale*, in *Cass. pen.*, 2011, p. 4509); S. Aterno - F. Cajani - G. Costabile - M. Mattiucci - G. Mazzaraco (a cura di), *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Experta, Forlì, 2011, p. 411.

[14] G. Costabile, *Computer forensics e informatica investigativa alla luce della legge n. 48 del 2008*, in *Ciberspazio e diritto*, 2010, p. 465 ss.; L. Lupária - G. Ziccardi, *Investigazione penale e tecnologia informatica*, 2007, Giuffrè, Milano, p. 136.

[15] Attraverso l'analisi forense è possibile effettuare una verifica tecnica anche su tutte quelle parti apparentemente vuote, che potrebbero nascondere *file* o frammenti di *file* cancellati e quindi assumere un'importanza decisiva nell'ambito dell'indagine penale (S. Aterno, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. mer.*, 2013, p. 955).

1-*bis*, 352, comma 1-*bis*, 354, comma 2, c.p.p.);
– l'obbligo di impedire l'alterazione successiva del dato originale (artt. 244, comma 2, 247, comma 1-*bis*, 352, comma 1-*bis*, 354, comma 2, c.p.p.);
– la formazione di una copia che assicuri la conformità del dato informatico all'originale (art. 354, comma 2, c.p.p.);
– la prescrizione di assicurare la non modificabilità della copia del documento informatico (la c.d. catena di custodia disciplinata dall'art. 254-*bis* c.p.p.);
– la garanzia dell'installazione di sigilli informatici sui documenti acquisiti (c.d. *hash*, previsto dall'art. 260 c.p.p.)[16].

Nella complessità e delicatezza di un sistema processuale in continua evoluzione, non si può trascurare lo scetticismo di coloro che, dinanzi al dilagare incessante della prova digitale, paventa la possibile retrocessione del contraddittorio per la formazione della prova, che rischia di essere relegato a vaglio sulla genuinità del dato informatico[17].

2. Ispezione e perquisizione informatica

Per ispezione si intende l'atto con il quale si esamina una persona, una cosa od un luogo, allo scopo di acquisirne conoscenza e di rilevare le tracce o gli effetti del reato[18].

Si tratta di un mezzo di ricerca della prova che sembra maggiormente attinente al reato informatico e alle sue caratteristiche, specie se si considera che l'ispezione di luoghi e di cose ha generalmente per oggetto beni tendenzialmente immateriali o deteriorabili, facilmente inquinabili o comunque volatili.

---

[16] S. De Flammineis, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in Sistema pen., 8 marzo 2024.

[17] R. E. Kostoris, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in F. Ruggieri – L. Picotti (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Atti del Convegno Como, 21-22 maggio 2010, Torino, Giappichelli, 2011, p. 181.

[18] La differenza fra tracce ed effetti è nota: le prime consistono in segni, macchie o impronte direttamente o indirettamente prodotte dalla condotta delittuosa su una determinata cosa o in un determinato luogo; i secondi, invece, sembrano «richiamare alla mente le conseguenze o alterazioni di natura contundente, percussiva, ustionante, abrasiva, perforante, effrattiva che la stessa condotta può aver determinato su luoghi, cose o persone» (P. Felicioni, voce *Prova scientifica*, in *Dig. disc. pen.*, Agg. VIII, Utet, Torino, 2014, p. 611). In argomento v. inoltre P. Moscarini, *Lo statuto della "prova scientifica" nel processo penale*, cit., p. 649; P. Moscarini, voce *Ispezione* (diritto processuale penale), in *Enc. dir.*, Agg., vol. II, Giuffrè, Milano, 1998, p. 464; G. Nicolucci, *L'assunzione di nuove prove in dibattimento: il caso dell'ispezione*, in *Giur. mer.*, 2001, p. 573.