Prova digitale tra garanzie costituzionali, prassi operative e “copia-mezzo”

L’avvento della *Digital Forensics* ha imposto una transizione irreversibile ed inarrestabile nel paradigma investigativo, la ricostruzione del fatto storico è migrata in un’istante dalla tradizionale (e spesso fallibile) prova dichiarativa verso un modello di accertamento scientifico del dato.

In questo scenario, la Legge 48/2008 ha rappresentato lo spartiacque normativo necessario per recepire la Convenzione di Budapest, ma il suo limite è emerso chiaramente nella prassi: se da un lato ha codificato il “come” (blindando l’acquisizione tramite protocolli di integrità e immodificabilità, come l’hashing e la catena di custodia), dall’altro ha lasciato una zona d’ombra sul “cosa” sia legittimo acquisire e, soprattutto, sul limite temporale della detenzione del dato e gestione dello stesso. È proprio in questo vuoto che si inserisce l’elaborazione giurisprudenziale della “copia-mezzo”.

Ontologicamente, la copia-mezzo non rappresenta l’oggetto del sequestro in sé, ma si configura come una “copia servente” (il mezzo): uno strumento tecnico-giuridico volto a bilanciare l’esigenza investigativa con il diritto alla restituzione del “contenitore” fisico (smartphone, workstation, notebook etc.) all’avente diritto.

Si assiste, di fatto, alla dematerializzazione della perquisizione, che si sposta dal piano fisico a un ambiente digitale controllato. Tuttavia, come evidenziato dalla Suprema Corte[1] , questa copia speculare genera un paradosso investigativo: essa cristallizza una massa di dati “indistinti e magmatici”, un vero e proprio “ecosistema digitale”[2] che,

ab origine, è privo di una funzione probatoria definita e contiene la totalità della vita privata dell'interessato. La legittimità della ritenzione di tale massa è dunque subordinata a un vincolo temporale e finalistico stringente: il "tempo strettamente necessario"[3] per l'attività di *filtering* e selezione dei dati pertinenti.

Oltrepassare tale limite significa snaturare l'istituto: senza una selezione mirata, la copia-mezzo smette di essere uno strumento probatorio e diventa una forma di sequestro esplorativo indiscriminato, eludendo il precetto dell'art. 253 c.p.p. e trasformando l'indagine in una pericolosa attività di *fishing expedition* (pesca a strascico) vietata dal nostro ordinamento.

Il dato comunicativo tra "documento" e "corrispondenza": la nuova barriera della Corte Costituzionale

La complessità epistemologica della "copia-mezzo", appena introdotta, raggiunge, probabilmente il suo apice critico, quando l'analisi si sposta dai file statici al dominio della comunicazione digitale, sempre più diffusa nella nostra quotidianità.

La rivoluzione interpretativa innescata da qualche anno dalla Corte Costituzionale (sent. 170/2023) e dalle Cassazione [4] ha scardinato la prassi consolidata che considerava SMS, e-mail e messaggistica istantanea (WhatsApp, Telegram) alla stregua di meri "documenti" una volta archiviati nella memoria del dispositivo. Si è oggi affermato un principio di "ultra-vitalità ed attualità della corrispondenza": il dato comunicativo, finché conserva un carattere di attualità per gli interlocutori e non degrada a mero reperto storico, rimane protetto dall'inviolabile scudo dell'art. 15 della

Costituzione.

Questa ontologia del dato impone un radicale cambio di passo: l'acquisizione non può più avvenire tramite un generico decreto di sequestro probatorio (art. 253 c.p.p.), ma esige un atto motivato che rispetti le forme dell'art. 254 c.p.p., con tutte le garanzie che ne conseguono in termini di riserva di giurisdizione. Sul piano operativo, l'impatto per la Polizia Giudiziaria e per gli specialisti di *Digital Forensics* è, per certi versi, dirompente. La prassi dell'ispezione immediata del contenuto del dispositivo al momento del sequestro – volta a ricercare "a caldo" elementi utili – diviene un terreno minato.

L'operatore deve oggi limitarsi alla mera apprensione fisica o alla duplicazione integrale (bit-stream image) del supporto, astenendosi da qualsiasi attività di cognizione diretta del contenuto comunicativo prima dell'emissione di un decreto specifico. Ogni incursione non autorizzata nel "flusso del pensiero" cristallizzato nei messaggi rischia di generare un'inutilizzabilità patologica della prova, rendendo vano lo sforzo investigativo.

A questo scenario interno si sovrappone la pressione della giurisprudenza sovranazionale. La Corte di Giustizia UE (sent. C-548/21)<[5] sta spingendo verso un modello in cui l'accesso ai dati digitali sia subordinato al controllo preventivo di un giudice o di un'autorità amministrativa indipendente.

Questo orientamento mette in crisi l'architettura del nostro Codice, laddove il Pubblico Ministero, pur essendo parte dell'Autorità Giudiziaria, è percepito dalla giurisprudenza europea come parte processuale priva di quella terzietà assoluta necessaria per autorizzare l'intrusione massiva nella sfera privata garantita dai moderni smartphone. In sintesi, la "copia-mezzo" non è più solo un contenitore tecnico, ma un sacrario di diritti che la tecnica forense deve imparare a maneggiare con estrema cautela procedurale.

Il mosaico delle prassi: la risposta resiliente delle Procure al vuoto normativo

In attesa di un intervento organico del legislatore – con lo sguardo rivolto al dibattito sul DDL S. 806 (approvato) – C.1822 (in corso di esame in commissione)[6]– il panorama nazionale si presenta come un laboratorio a cielo aperto.

Le Procure italiane, consapevoli che la "copia-mezzo" non può più essere "negata" ma va gestita[7], hanno elaborato linee guida (direttive) [8] che tentano di sintetizzare due esigenze opposte: il rigore del "Giusto Processo – Fair Trial" e l'efficacia dell'azione di contrasto al crimine.

L'evoluzione della *Digital Forensics* nel panorama giudiziario italiano ha imposto l'adozione di protocolli d'azione che, pur in assenza di una riforma organica del codice di rito, garantiscano l'integrità del dato e la tenuta costituzionale delle indagini, in particolare dall'analisi delle direttive emanate dalle principali Procure della Repubblica, emerge innanzitutto un solido nucleo di tratti comuni, che costituiscono ormai il "minimo denominatore" della disciplina.

Tutte le direttive/circolari concordano sulla natura strumentale e temporanea del sequestro del supporto fisico: lo smartphone o il PC non sono più il fine dell'apprensione, ma il mero veicolo per giungere alla formazione della "copia-mezzo". Il riconoscimento della copia forense come unico ambiente di analisi investigativa e l'obbligo di restituzione immediata dell'originale rappresentano il pilastro di un sistema che tenta di rispettare il principio di proporzionalità, limitando l'invasività del sequestro ai soli tempi tecnici di duplicazione *bit-stream*.

Tuttavia, superata questa base metodologica, il panorama si frammenta in un mosaico di prassi e direttive che riflettono

diverse interpretazioni del bilanciamento tra efficienza e garanzie. Questo sforzo di auto-regolamentazione ha prodotto modelli d'eccellenza che nelle loro similitudini e differenze meritano un'analisi di dettaglio.

La **Procura di Trento**, ad esempio, declina il tema con un marcato accento sulla protezione dei dati personali. La sua direttiva si distingue per una lotta serrata contro la proliferazione dei cosiddetti "archivi di massa paralleli". In questa visione, la Polizia Giudiziaria non deve trattenere duplicati informali che potrebbero trasformarsi in banche dati permanenti al di fuori del controllo giudiziario. Il focus trentino è quasi "ecologico": una volta selezionato il dato pertinente (chat, mail, messaggistica), tutto ciò che è eccedente deve essere rimosso, per evitare che la vita privata di indagati o terzi rimanga cristallizzata nei server degli uffici investigativi senza una reale necessità processuale.

Spostandoci verso il modello adottato dalla **Procura di Bari**, l'attenzione si sposta sul rigore procedurale e sulla compartimentazione delle competenze. Qui, la differenza sostanziale risiede nella "neutralizzazione" tecnica della Polizia Giudiziaria nella fase di analisi profonda. Agli operanti è richiesto un ruolo di primi soccorritori (*First Responders*): devono isolare il dispositivo e assicurarne l'integrità. La fase successiva, quella della creazione della copia e del *filtering*, viene idealmente sottratta alla discrezionalità investigativa per essere affidata al tecnicismo dei consulenti ex art. 359 c.p.p. L'uso della crittografia obbligatoria per la copia-mezzo, con chiavi consegnate in busta chiusa al PM, eleva lo standard di sicurezza a un livello quasi notarile, rendendo Bari l'avamposto della "certificazione del dato".

Un approccio radicalmente diverso è quello che emerge dalla **Procura di Roma**, la quale rivendica con forza l'autonomia investigativa del Pubblico Ministero. Mentre la tendenza europea spinge per un controllo preventivo del giudice, il

modello romano difende la prerogativa dell'organo inquirente di disporre il sequestro senza autorizzazione del GIP, a patto che il decreto sia supportato da una motivazione "chirurgica". Roma non punta sulla distruzione immediata o sulla delega a terzi, ma sulla qualità della perimetrazione investigativa: è il magistrato che, definendo parole chiave e archi temporali, deve farsi garante della pertinenza, mantenendo però la rapidità d'azione tipica della fase inquirente.

Infine, le realtà di **Torino e Cagliari** introducono una variabile fondamentale per la tenuta del futuro processo: la "copia di sicurezza". Queste Procure hanno compreso che la cancellazione eccessivamente zelante dei dati non pertinenti potrebbe paradossalmente ledere il diritto di difesa. Torino, in particolare, si distingue per l'adozione di standard tecnologici elevati, come l'uso dei nastri magnetici LTO, per conservare una copia integrale in un "limbo" protetto.

Questa scelta operativa garantisce la parità delle armi, permettendo alla difesa di accedere, se autorizzata, a quella massa magmatica originaria che la PG potrebbe aver scartato, ma che potrebbe contenere elementi a discarico. Cagliari, dal canto suo, specifica con precisione i provvedimenti di distruzione nel caso di assenza di esigenze conservative, ma ribadisce che tale atto deve sempre fare salvo il diritto al contraddittorio, ponendosi come sintesi equilibrata tra il rigore della privacy di Trento e le esigenze garantiste di Torino.

In conclusione, sebbene il "punto di partenza" (la copia forense) sia identico per tutte, il "punto di arrivo" varia significativamente: dalla distruzione cautelativa di Trento alla conservazione archivistica di Torino, passando per il blindaggio tecnico di Bari e il pragmatismo inquirente di Roma. Questo scenario delinea un'Italia a più velocità, dove la *Digital Forensics* non è solo una disciplina tecnica, ma un vero e proprio esercizio di ingegneria costituzionale applicata.

Selezione del dato e crisi del contraddittorio nell'analisi forense

Il passaggio dalla "massa magmatica" della copia-mezzo alla formazione della prova utilizzabile in dibattimento non è un'operazione neutra, ma un processo di distillazione tecnicamente insidioso e giuridicamente parziale, invero, se la creazione della copia forense garantisce l'integrità del reperto, è nella fase di **selezione** che si gioca il destino del processo.

Tuttavia, gli strumenti oggi utilizzati per setacciare i gigabyte di vita digitale contenuti in uno smartphone si rivelano spesso inadeguati o, peggio, forieri di pericolosi *bias* investigativi[9].

L'uso delle keyword (parole chiave), pur essendo il metodo più diffuso, manifesta limiti strutturali che rasentano la fallacia metodologica. Da un lato, l'utilizzo di termini troppo generici genera un "rumore di fondo" che viola il principio di proporzionalità, trascinando nel fascicolo processuale stralci di vita privata del tutto irrilevanti. Dall'altro, l'impiego di termini eccessivamente specifici rischia di fallire l'obiettivo, non intercettando comunicazioni occultate dietro linguaggi gergali o criptici.

Nel gergo dei narcotrafficanti, termini come *"bamba"* o *"bimba" / "ananas"* o "*banane*" sostituiscono la sostanza stupefacente, rendendo una ricerca testuale standard del tutto inefficace. La selezione, dunque, non è mai un atto puramente meccanico, ma un'operazione semantica complessa che richiede un'interpretazione contestuale che la macchina, da sola, non può fornire. Peraltro, un "sistema" complesso e cronologico, basato su una tempistica stringente come quello della "copia-mezzo" non sempre permette di apprezzare compitamente quali

siano i termini gergali o criptici se non dopo una peculiare analisi dell'intero "patrimonio digitale" acquisito all'indagine. Il cuore della criticità risiede nella natura unilaterale di questa attività.

La prassi attuale delega la delicata fase del *filtering* al consulente tecnico del PM o alla Polizia Giudiziaria, spesso confinando la difesa in un ruolo meramente passivo. Sebbene l'acquisizione della copia sia tecnicamente ripetibile (art. 359 c.p.p.), la selezione dei dati avviene in un cono d'ombra dove il contraddittorio è assente. Il rischio è la cristallizzazione di un quadro probatorio parziale: se l'accusa seleziona solo i frammenti che confermano l'ipotesi di reato, la verità processuale risulterà irrimediabilmente zoppa.

In questo solco si inseriscono le proposte del DDL 806, già prima richiamato e le riflessioni della dottrina più avanzata, che premono per una "proceduralizzazione" della selezione. L'obiettivo è anticipare il contraddittorio già nella fase di definizione dei criteri di ricerca.

Trasformare l'accertamento da consulenza unilaterale in una sorta di "perizia garantita" – magari attraverso lo schema dell'incidente probatorio (art. 360 c.p.p.) – permetterebbe alla difesa di interloquire su *cosa* cercare e con *quali* strumenti, garantendo che l'indagine non diventi una ricerca a senso unico[10]. Un aspetto troppo spesso trascurato è il pericolo legato alla distruzione della copia-mezzo dopo la selezione iniziale. Operativamente, ogni indagine vive di una "escalation investigativa": elementi emersi mesi dopo il sequestro potrebbero dare un significato nuovo a dati inizialmente scartati.

Se la copia integrale viene distrutta in nome di una privacy malintesa o di una prassi frettolosa, si preclude definitivamente la possibilità di correlare nuovi indizi a vecchi dati, mutilando sia la capacità di accertamento della

verità da parte del PM, sia il diritto della difesa di ricercare elementi a discarico emersi in un secondo momento. La sfida della moderna *Digital Forensics* è dunque questa: proteggere la privacy senza accecare la giustizia, e garantire la prova senza sacrificare il diritto alla difesa nel nome di un'efficienza puramente formale.

Oltre la tecnica: verso un'etica della prova digitale e il nuovo ruolo del giudice

Il percorso fin qui delineato rende evidente come il quadro attuale non sia più sostenibile attraverso il solo strumento delle prassi circolari o dell'auto-regolamentazione delle singole Procure. Siamo giunti a un punto di rottura epistemologico che esige un intervento legislativo organico e coraggioso. In questo senso, il DDL 806 non rappresenta solo una proposta normativa, ma una vera e propria necessità di civiltà giuridica: il passaggio verso un controllo giurisdizionale preventivo (affidato al GIP) sul sequestro dei dispositivi elettronici non è più procrastinabile e richiede una presa di posizione che permetta di uscire dalla situazione "a macchia di leopardo" in cui oggi gli addetti ai lavori si trovano ad operare[11].

Equiparare l'intrusione digitale alle intercettazioni telefoniche significa finalmente riconoscere che uno smartphone non è un semplice oggetto, ma l'estensione digitale dell'anima e della libertà della persona.

Sottrarre al Pubblico Ministero la gestione esclusiva di una fase così pervasiva risponde non solo alle pressanti sollecitazioni della giurisprudenza sovranazionale (Corte EDU e CGUE), ma riporta l'equilibrio tra poteri al centro del processo penale. La "copia-mezzo" deve cessare di essere un'appendice tecnica gestita unilateralmente per diventare il

fulcro di una procedura garantita, dove la duplicazione avvenga in un contraddittorio effettivo e il “congelamento” del dato sia funzionale a una selezione partecipata, e non a un’acquisizione indiscriminata.

In questa nuova architettura della prova, il tecnico forense non è più solo un estrattore di bit, ma un custode di garanzie. La sfida del futuro legislatore sarà quella di codificare un sistema capace di prevenire le cosiddette “pesche a strascico” (*fishing expeditions*) nella vita privata dei cittadini, garantendo che ogni byte acquisito rispetti rigorosamente i canoni di pertinenza e proporzionalità.

La “copia-mezzo”, in definitiva, non può e non deve più essere considerata un mero artefatto transitorio. Essa è lo specchio di una metamorfosi che vede il processo penale misurarsi con la complessità dell’era digitale, solo attraverso una sintesi equilibrata tra rigore tecnico, controllo del giudice e centralità del contraddittorio, potremo assicurare che la ricerca della verità non avvenga mai a discapito dei diritti fondamentali, trasformando la *Digital Forensics* da strumento di potenziale oppressione a presidio di legalità e giustizia.

Se il dato è il “nuovo petrolio”, la procedura penale deve esserne il raffinato sistema di controllo ambientale, per evitare che la fuoriuscita indiscriminata di informazioni personali inquini irrimediabilmente le basi dello Stato di Diritto.

Note:

[1] Cass. pen. Sez. VI, Sent., (ud. 09-12-2020) 19-02-2021, n. 6623 – Sez. VI, n. 34265 del 22/9/2020, Aleotti, Rv. 279949; ma per riferimenti alle modalità operative si rinvia anche a Sez. VI, n. 13165 del 4/3/2020, Scagliarini, Rv. 279143.

[2] Un vero e proprio “ecosistema digitale” che, nella realtà tecnologica odierna, risulta ulteriormente esaltato dal fenomeno della sincronizzazione permanente. Quest’ultima

trasforma il dato da elemento statico, confinato nel singolo hardware, in un flusso ubiquo che si concretizza nella circolazione bidirezionale tra dispositivi fisici (smartphone, tablet, PC) e infrastrutture cloud. Ne deriva che l'ecosistema del soggetto non è più una "scatola" chiusa, ma un reticolo di informazioni costantemente aggiornate e speculari, dove il confine tra memoria locale e archivio remoto sfuma, rendendo la cristallizzazione investigativa ancora più complessa e invasiva.

[3] Cass. Pen., Sez. VI, n. 543/2026.

[4] In particolare: Sez. VI, n. 34265 del 22/9/2020, Aleotti, Rv. 279949 – Cass. pen. Sez. VI, Sent., (ud. 21-05-2024) 30-07-2024, n. 31180.

[5] https://archiviopenale.it/corte-di-giustizia-dell-unione-europea-(grande-camera)-4-ottobre-2024-causa-c-548-21/contenuti/29682

[6] https://www.senato.it/leggi-e-documenti/disegni-di-legge/scheda-ddl?did=57327

[7] Già citata in nota 3 – Cass. Pen. Sez. VI, sentenza n. 543 depositata l'8 gennaio 2026.

[8] Dirette alla PG e al PM.

[9] Talvolta aggravati dall'utilizzo sempre più spinto di sistemi di intelligenza artificiale. In merito rimando ad altri miei articoli e ad altri contributi reperibili in rete: "Pier-Luca Toselli, AI e digital forensics".

[10] Sui lavori in corso in Parlamento, rinvio a questo link: https://www.camera.it/leg19/126?leg=19&idDocumento=1822
dove si possono leggere, nella sezione Attività conoscitiva, le audizioni informali, tra gli altri, di Giovanni Melillo,

procuratore nazionale antimafia e antiterrorismo; Cesare Parodi, presidente dell'Associazione nazionale magistrati; Francesco Cajani, Sostituto Procuratore della Repubblica presso il Tribunale di Milano; Maurizio De Lucia, Procuratore della Repubblica di Palermo.

[11] Si pensi alle situazioni investigative che interessano più Procure con diverse direttive.

Profilo Autore

Sono un ufficiale di polizia Giudiziaria che ha maturato un'esperienza ormai trentennale nel settore della sicurezza e delle investigazioni, con specifico riferimento negli ultimi 8 anni alla digital forensic per la quale ho conseguito la qualifica di Computer Forensic e Data Analysis . L'esperienza ha anche permesso di consolidare ed affinare una solida preparazione tecnico-giuridica sia nel settore delle investigazioni in genere sia in quello più prettamente informatico. Sono stato docente nell'ambito del Master Executive di II livello in Criminologia e Cyber Security – Modulo 7: Lotta al Crimine organizzato (Master Sida – Fondazione INUIT Tor Vergata).

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/copia-mezzo/