

Fine della copia integrale e del sequestro a “strascico”: barriere crittografiche, garanzie costituzionali e giurisprudenza

Alla 14^a Cyber Crime Conference (Roma, 6-7 maggio 2026) Pier-Luca Toselli ha ricostruito il nuovo equilibrio fra esigenze investigative e tutela dei diritti nel sequestro probatorio dei dispositivi digitali. Fra le pronunce più recenti della Cassazione, le direttive delle Procure e il DDL A.C. 1822 / A.S. 806, prende forma un sistema che archivia la cosiddetta “pesca a strascico”, ma la cui disciplina operativa resta tutt’altro che lineare.

Dalla “pesca a strascico” alla copia mirata

Pier-Luca Toselli, esperto senior in *digital forensics* e investigazioni digitali, con quasi trentotto anni di esperienza nella Guardia di Finanza e oggi libero professionista, ha aperto il suo intervento con un richiamo storico: gli albori della Legge 48/2008. Prima di quella legge le perquisizioni informatiche si risolvevano spesso in un “sequestro indiscriminato”. Si entrava in casa di un soggetto, si portava via tutto ciò che lampeggiava (compresa, paradossalmente, la spia del frigorifero) e si analizzava poi in laboratorio, con calma.

Quella stagione, ha osservato Toselli, è oggi definitivamente chiusa. Il punto di svolta porta una data precisa: la **Cass. Pen. Sez. VI n. 2234 del 20 gennaio 2026**, che ha consolidato

un orientamento già delineato negli anni precedenti. In tema di sequestro probatorio di dati contenuti in dispositivi informatici o telematici, il decreto del Pubblico Ministero deve contenere specifica motivazione sulla proporzionalità e adeguatezza della misura, illustrando le ragioni che rendono necessario un sequestro esteso e onnicomprensivo e indicando sia le informazioni ricercate sia i criteri di selezione del materiale archiviato nel dispositivo.



*La fine della copia integrale e del sequestro a “strascico”:
Cass. Pen. Sez. VI n. 2234 del 20 gennaio 2026*

Soprattutto, “il sequestro probatorio non può assumere valenza meramente esplorativa”: non essendo, nel disegno del legislatore, un mezzo di ricerca della notizia di reato, ma solo della sua conferma.

I principi consolidati dalla giurisprudenza

Sui principi che oggi presidiano l’acquisizione probatoria digitale Toselli ha richiamato in particolare la **Cass. Pen. Sez. VI n. 24671 del 4 luglio 2025** e la **Cass. Pen. Sez. II n. 33657 del 13 ottobre 2025**:

- illegittimità del sequestro indiscriminato;
- principio di proporzionalità e adeguatezza;
- divieto di acquisizione esplorativa;
- criteri di selezione e limiti temporali;
- meccanismo di copia-mezzo e restituzione.

L’insieme di questi vincoli viene sintetizzato dal relatore con l’acronimo **TPA**: temporaneità, proporzionalità e adeguatezza del sequestro. Per anni, ha osservato, “siamo stati abituati alla ricerca del reato a seguito dell’esame di tutte le prove acquisite in un determinato procedimento”: capita ancora che da una perquisizione per evasione fiscale si arrivi a fattispecie del tutto diverse. Quel paradigma esplorativo è oggi giuridicamente insostenibile.

La selezione rapida dei dati e la sentenza 170/2023

Sul versante della tempistica, Toselli ha richiamato la **Corte Costituzionale n. 170 del 2023**, che impone, nel caso del sequestro probatorio di dispositivi informatici, una rapida selezione dei dati e la celere restituzione al titolare di tutto ciò che non è pertinente. Lo ha poi collegato alla **Cass. Pen. Sez. VI n. 543 dep. 8 gennaio 2026**, secondo cui la valenza costituzionale del principio di proporzionalità non consente “zone franche”: la proporzione temporale del vincolo reale deve essere valutata già al momento dell’adozione della misura cautelare reale, nei limiti di una ragionevole previsione.  *La fine della copia integrale e del sequestro a “strascico”: Cass. Pen. Sez. VI n. 543 dep. 8 gennaio 2026*

In questo quadro la **Cass. Pen. Sez. III n. 3350 del 28 gennaio 2026** ha precisato i contenuti minimi della motivazione: il PM deve indicare specificamente, anche in modo conciso, le ragioni che rendono necessaria la limitazione della disponibilità dei dati, le informazioni ricercate e i criteri di selezione rispetto al reato contestato. La stessa pronuncia ha escluso un termine perentorio per la selezione.  *La fine della copia integrale e del sequestro a “strascico”: Cass. Pen. Sez. III n. 3350 del 28 gennaio 2026*

Sarebbe inevitabilmente approssimativo, condizionato da variabili tecniche come la difficoltà di accesso o il reperimento di consulenti; ha però confermato che la durata del sequestro deve essere limitata al tempo strettamente necessario alle operazioni tecniche, lasciando all’interessato la facoltà di richiedere la restituzione del dispositivo dopo un periodo congruo (indicativamente dieci giorni) e di proporre opposizione ex art. 263 c.p.p. in caso di rifiuto.

Il messaggio operativo è netto: non è più pensabile sequestrare dispositivi, riporli in un armadio e analizzarli con calma nei sei mesi delle indagini preliminari. La

selezione deve avvenire in tempi rapidi, espellendo dal compendio digitale tutto ciò che non riguarda il procedimento.

Copia-mezzo e copia-fine: il modello operativo

Una parte centrale dell'intervento è dedicata alla distinzione fra **copia-mezzo** e **copia-fine**, che oggi regge l'intera procedura. La copia-mezzo è la copia forense *bit a bit* del dispositivo (la classica copia fisica, quando tecnicamente possibile): sulla sua base viene poi effettuata la selezione dei dati pertinenti. Da quella selezione nasce la copia-fine, ovvero il sottoinsieme di elementi rilevanti per il procedimento, destinato al dibattimento. La copia integrale, in altre parole, non è più la prova finale ma uno strumento funzionale alla selezione dei dati pertinenti e alla restituzione del dispositivo.

Il valore probatorio della copia-mezzo è garantito dall'integrità del dato, verificata tramite *hash*. È proprio sulla fase di selezione, però, che si annidano le maggiori criticità pratiche: la fallibilità di una ricerca per parola chiave o per data è evidente per chiunque abbia esperienza del settore, e la lettura incrociata dei dati richiede inevitabilmente il contributo conoscitivo sia dell'accusa sia della difesa.

Le criticità: tecniche e giuridiche

Sul piano tecnico Toselli ha richiamato un insieme di nodi ormai strutturali:

- **collaborazione della persona:** senza il contributo dell'utente, la crittografia rende oggi spesso impossibile un'acquisizione piena dei dati e la successiva selezione;
- **forme di sicurezza dei dispositivi,** sempre più

- stratificate;
- **utilizzo diffuso della crittografia;**
- **eterogeneità di modelli e sistemi operativi.**

Sul piano giuridico, invece, le criticità nascono dal continuo attrito fra le esigenze investigative e i principi TPA. In un contesto in cui, come ha rilevato con franchezza il relatore, “tante volte la legge viene fatta dalla giurisprudenza”, e ciò non è del tutto corretto.

Il mosaico delle direttive delle Procure

A complicare il quadro si sono aggiunte le direttive emanate da diverse Procure (Torino, Trento, Roma, Cagliari, Bari) per orientare l'attività della polizia giudiziaria nei rispettivi territori. Pur con sfumature diverse, queste direttive condividono alcuni tratti di fondo:

- il riconoscimento dell'importanza delle prove digitali e della *copia forense* a supporto delle indagini;
- una sequenza procedurale tipica che prevede sequestro del dispositivo, formazione della copia forense, immediata restituzione del dispositivo, qualificazione del sequestro dell'originale come strumentale e temporaneo, esecuzione dell'analisi investigativa sulla copia forense e successiva selezione che porta prima alla copia-mezzo e poi alla copia-fine;
- il rispetto del principio di proporzionalità e pertinenza, il divieto di “mandato esplorativo”, la gestione attenta dei dati personali e sensibili, la gestione delle notizie di reato diverse emerse incidentalmente e il ruolo centrale del Pubblico Ministero.

Il problema, ha rilevato Toselli, è che pratiche e qualificazioni cambiano da Procura a Procura: a oggi non è chiaro nemmeno se queste operazioni debbano essere svolte come accertamenti irripetibili ex art. 359 c.p.p. oppure con le garanzie dell'art. 360 c.p.p.. “Se stamattina dicevamo che

servirebbe una certa omogeneizzazione a livello europeo”, ha osservato, “probabilmente non l’abbiamo neanche a livello regionale”.

Messaggistica e corrispondenza: il riallineamento giurisprudenziale

Un capitolo specifico è stato dedicato alla qualificazione giuridica della messaggistica. Toselli ha richiamato la **Cass. Pen. Sez. II n. 33657 del 13 ottobre 2025**, secondo cui è illegittimo il decreto di sequestro probatorio di un telefono cellulare con il quale il Pubblico Ministero acquisisca la totalità dei messaggi, filmati e fotografie ivi contenuti, senza indicare le ragioni per le quali, ai fini dell’accertamento dei reati ipotizzati, si renda imprescindibile l’integrale verifica di tutti i predetti dati e si giustifichi, nel rispetto del principio di proporzionalità, un così penetrante sacrificio del diritto alla segretezza della corrispondenza.

La svolta sostanziale è arrivata con la **Corte Costituzionale n. 170 del 2023**, che ha stabilito come lo scambio di messaggi elettronici (*e-mail*, SMS, WhatsApp) rientri pienamente nella nozione di “corrispondenza” tutelata dall’art. 15 della Costituzione: la natura di corrispondenza persiste anche dopo la ricezione (la cosiddetta “dimensione statica”), finché il messaggio conserva un carattere di attualità e interesse per i corrispondenti.

Su questa traccia si è mossa la **Cass. n. 25549 del 15 maggio 2024**, che ha recepito l’orientamento della Consulta affermando la persistenza della natura di corrispondenza anche dopo la ricezione e ricondotto il sequestro alle forme dell’art. 254 c.p.p.. Come ha ricordato il relatore, l’art. 254 c.p.p. vieta alla polizia giudiziaria di accedere al contenuto dei messaggi nel momento stesso del sequestro: il dispositivo deve essere consegnato all’autorità giudiziaria, unica legittimata a

verificarne il contenuto. La **Cass. Pen. Sez. VI n. 13585/2025** ha poi precisato che l'accesso ai dati di un dispositivo informatico a fini di indagine penale richiede il controllo di un giudice o di un organo amministrativo indipendente e terzo rispetto all'organo richiedente.

Toselli ha tuttavia segnalato il nodo operativo: stabilire quando un messaggio conservi un "carattere di attualità e interesse per i corrispondenti" è una valutazione che rischia di scivolare nel terreno strumentale e si presta a letture divergenti fra accusa e difesa. Il parallelo è quello, ben noto a chi ha fatto *digital forensics* da prima, dell'antica diatriba sull'e-mail "aperta" e "chiusa": una distinzione che dal lato informatico è sempre stata, in fondo, un nonsenso.

Le prospettive di riforma: il DDL A.C. 1822 / A.S. 806

L'attuale quadro normativo (artt. 253 e 254 c.p.p., L. 48/2008) è ormai considerato inadeguato a disciplinare il sequestro dei dispositivi informatici e le indagini sui dati digitali, e lascia ampi margini di discrezionalità e incertezza. In questo contesto si inserisce la proposta comune sul **DDL A.C. 1822 / A.S. 806**, che mira a colmare le lacune introducendo nel codice di procedura penale il nuovo **art. 254-ter** dedicato specificamente al sequestro di dispositivi, sistemi informatici, dati e comunicazioni. La proposta prevede una riserva di giurisdizione per il sequestro del dispositivo (decreto motivato del GIP su richiesta del PM, con deroga per urgenza e successiva convalida) e introduce discipline distinte per l'acquisizione e l'analisi dei dati comunicativi e non comunicativi.

L'impianto della riforma, ha riassunto Toselli, ruota intorno ad alcuni assi principali:

- **semplificazione delle procedure e ampliamento**

dell'utilizzabilità delle prove digitali, ormai strategiche in ogni indagine;

- **equilibrio fra tutela dei diritti ed efficacia investigativa;**
- **diritto al contraddittorio e ruolo della difesa,** con partecipazione effettiva non solo nella fase di analisi ma anche in quella di acquisizione della prova digitale.

Su quest'ultimo punto Toselli si è soffermato con particolare attenzione. La difesa dovrebbe disporre di controllo tecnico tempestivo, di accesso alle copie forensi dei dati e della possibilità di contestare ricostruzioni non corrispondenti.

A questo si affianca la proposta di un **rafforzamento del ruolo del GIP** in passaggi critici: accesso a dati remoti (*Cloud*) subordinato a previa autorizzazione del GIP, data la delicatezza e l'ampiezza di tali dati; controllo *ex ante* o validazione giudiziale *ex post* per la deroga alla duplicazione ordinaria ex art. 254-ter co. 10 in caso di urgenza; introduzione di una fase partecipata post-duplicazione per la difesa e la persona offesa nella selezione dei dati operata dal PM; oppure, in alternativa, proroga del termine per l'esame e verbalizzazione accurata delle operazioni, con verifica e autorizzazione del giudice.

Sul versante della perquisizione informatica (art. 247 c.p.p.) la proposta normativa, nella sua attuale formulazione, lascerebbe il potere ancora in capo al Pubblico Ministero, con il rischio di eludere le nuove garanzie previste per il sequestro: la perquisizione digitale comporta di fatto una duplicazione non sorvegliata. Per questo si propone che ogni perquisizione di dispositivo digitale richieda previa autorizzazione del GIP, data la sua natura invasiva. Analogamente, in caso di perquisizioni o sopralluoghi d'iniziativa della polizia giudiziaria su dispositivi digitali ex artt. 352 e 354 c.p.p., la comunicazione al PM dovrebbe essere seguita da una richiesta di convalida al GIP, sullo schema dell'art. 254-ter co. 4.

Un “accertamento irripetibile anticipato”?

Toselli ha proposto una lettura suggestiva del nuovo assetto: la riforma, di fatto, configurerebbe una sorta di “**accertamento irripetibile anticipato**”. La perquisizione è l'atto irripetibile per antonomasia: consentire l'intervento della difesa fin dalle primissime fasi (eventualmente con l'ausilio di un consulente tecnico) diventa cruciale anche in sede di selezione dei dati, dove un identico *smartphone*, una identica messaggistica e una identica *chat* possono essere letti in modo radicalmente diverso a seconda dell'angolazione.

Il relatore ha però segnalato anche un nodo critico: la formulazione attuale rischia di tradursi in passaggi davanti al GIP non solo per la selezione copia-mezzo / copia-fine, ma anche per la legittimità stessa del sequestro (rispetto dei canoni TPA). Inoltre l'introduzione di termini molto stringenti (si parla di cinque giorni) appare poco realistica per chi conosce la procedura penale: in cinque giorni non si fanno neanche le notifiche, figurarsi un'attività di questo tipo davanti al GIP.

La riforma merita grande attenzione da parte di tutti gli operatori: è infatti già stato richiesto un intervento da numerose autorità, personalità accademiche, esperti e consulenti informatici. L'obiettivo non è “tifare” per l'accusa o per la difesa, ma evitare che le pieghe degli esiti politici portino a soluzioni che non aiutino né l'una né l'altra.

Una riflessione finale: oltre lo *smartphone*

In chiusura Toselli ha lasciato uno spunto destinato a pesare sulle prossime stagioni regolatorie e operative. Se questo è

il livello di complessità richiesto dalla disciplina del sequestro di uno *smartphone* o di un *hard disk* (oggetti che il relatore ha definito, *licentia poetica*, “qualcosa di morto”), è facile immaginare il salto di scala che attende gli operatori quando l’oggetto delle indagini sarà costituito da attacchi generati da intelligenza artificiale e da **agenti di intelligenza artificiale**: scenari in cui, come emerso nel corso della stessa Conference, già oggi non si è in grado di ricostruire con certezza nemmeno l’origine dell’attacco.

Il messaggio che esce dall’intervento è di lucida preoccupazione professionale. Il sistema italiano sta uscendo dalla stagione del “sequestro a strascico” grazie a una giurisprudenza coraggiosa, ma sta entrando in una fase in cui il dettaglio operativo (chi fa che cosa, in che termini, con quali garanzie e con quale controllo del GIP) resta ampiamente da scrivere. E le tecnologie corrono più veloci della procedura.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/copia-integrale-copia-mezzo/>